LM Series

Operation Manual

(Version 3.6)

iGuard®

Federal Communications Commission (FCC) Statement

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.
Increase the separation between the equipment and receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

CE

EMC DIRECTIVE 89/336/EEC (EN55022 / EN55024)

Trade Name : iGuard
Model No: FPS110 / LM

User's Notice

This manual contains detailed instructions and notes on the operation and use of the product. For your safety and benefit, read this manual carefully before using the product. Keep this manual in a handy place for quick reference.

Notes

- Some illustrations in this manual might be slightly different from the product.
- Certain options might not be available in some countries. For details, please contact your local dealer.

Important

Contents of this manual are subject to change without prior notice. In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the product.

Trademarks

- iGuard® is registered trademark of Lucky Technology Ltd.
- Microsoft® and Windows® are registered trademarks of Microsoft Corporation.
- Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

Table of Content

INSTALLATION

Proper planning is the key to successful implementation of any technology project. While the iGuard system is very easy to install and operate, there are some things to consider before you begin installation.

Pre-Installation Notes

- iGuard is designed for indoor use. If you plan to install it outdoors, be aware that exposing it to water, heat, or other harsh conditions can damage the device and it may not operate properly.
- Do not install iGuard next to heat sources or in direct sunlight.
- For iGuard units equipped with the optional fingerprint sensor, make sure the iGuard's back metal panel is properly grounded to *earth,* to prevent electrical impulses and shocks from affecting users and the iGuard units.
- To prevent electrical short-circuits or overload, power the iGuard independently with the power supply provided. Do not share the power with other device such as the electric door strike.
- For security and safety purposes, do not connect the door button to the iGuard terminals. Instead, connect it directly to the door strike, to avoid failure in case of a power outage or other emergencies.
- To increase the security level in access control applications, use the optional *Remote Relay* together with the iGuard unit. This device is sold separately, and it assures that malicious damage to or tampering with the iGuard does not result in a release of the electric door strike. Please refer to the Appendix for more information.
- Make sure the *Smartcard Company Code* is properly set ***before*** assigning any smartcard to users. This code is a configurable, 4-character code, which is to set your iGuard system apart from any other iGuard system. Any smartcard with a code that does not match is not recognized by the system. So once the smartcards have been assigned, do not change this Company Code. Please refer to the section "*Using the Web Browser → Administration → Terminal Setup → Code Setting"* for more information.

Installation

Determine the location(s) for installing iGuard, external *Remote Relay*, door strike and power supply line. Fasten the rear metal panel at the location where the iGuard unit will be installed. Connect the iGuard unit with the power supply provided.

Power Requirements & Back EMF issue

iGuard requires DC 12V / 500mA switching power supply. Sharing power with other devices, such as a door strike, is NOT recommended. This is because the potential back EMF (Electromotive Force) generated by the door strike may affect the iGuard. If it is necessary to share it with the door strike, a protection diode (1N4004 type) must be installed across the 12V power lines to the iGuard. Refer to the Connection Diagram in the Appendix for more information.

Warning: Use ONLY the power supply provided. Do not use other power supplies since this may lead to system failure, and poor or unreliable operation.

When deciding where to install…

iGuard is a wall-mounted unit with a miniscule footprint, and can be conveniently installed anywhere. However, for access control applications, it is recommended that the iGuard should be installed as close to the door as possible, so that the user can open the door within the timeout period, which is 5 seconds by default. Also note the following points:

- Make sure that air can circulate freely through the ventilation slots.
- Do not install the product next to heat-emitting sources, or in a place subject to direct sunlight and excessive dust.
- If fingerprint sensor is used, the Metal Back Panel must be grounded as shown in the following figure:-

Important: Mounting the Metal Back Panel (for iGuard with the optional fingerprint sensor). The iGuard comes with a metal panel for mounting on the wall. ***The panel must be grounded***. By doing so, the static electricity that users emit can be discharged directly to the ground. This will improve the fingerprint images of users.

Connect the Power & External Controls

iGuard provides easy-access terminals for connections to external controls, including Door Strikes, Door Sensor, Door Open Switch, and External Alarm.

Terminals	Description
1 & 2	**Power (12V DC)** The power requirement is 12V DC, 150mA (idle), 500mA (peak). Connect it to the power supply provided.
3, 4 & 5	**Door Strike** Terminal #3 & #4 are the normal-open (NO) pair, and terminal #4 & #5 are the normal-close (NC) pair. Connect the door strike to either pair of these terminals according to the type of the electric door strike.
6 & 7	**Door Sensor (Optional)** This pair provides iGuard the current status of the door (i.e., open / close). If the door is left open for over 10 seconds, iGuard will generate beep sounds to alarm.
8 & 9	**Reserved** Reserved for future use.
10 & 11	**External Alarm (Optional)** This pair is for the optional external alarm. In the case that the device is forced open and removed from the wall during operation, an internal case switch will connect this terminal pair, which can optionally sound an external alarm.
RS - 485 (for Remote Relay only)	**Remote Relay Connector** This is to connect the iGuard to the optional *Remote Relay* unit. Refer to the Appendix for more detail.
Wiegand	**Wiegand Connector** iGuard can be used as an Wiegand Reader. This Wiegand connector outputs the user ID to another Wiegand device in the standard 26-bit format.

Connect the Electric Door Strike

Connect the Electric Door Strike to the Terminal Pair #3 & #4 for normal-open type, or the pair #4 & #5 for normal-close type.

Internally, these terminals #3, #4 & #5 are connected directly to the internal relay, rating at 12V / 1Amp. If the door strike is within this current limit, it can be directly connected to these terminals. If the current rating is above 1 Amp, the Remote Relay must be used (to be discussed in the Appendix).

More details about the door strike connection are given in the connection diagrams in the Appendix.

The administrator should examine each door that is to be controlled, and determine the type of door (wood, glass, or metal), the direction it swings, the desired direction to be controlled (unless the unit will authenticate both directions), and the type of frame (wood or metal). This information will be helpful for determining the type of lock that is to be used with the iGuard. Please consult the dealer for more information about magnetic locks, electric strikes, and other door hardware.

If the system is used solely for Time Attendance purposes, these terminals can be left disconnected.

Connect the Network

iGuard is designed to be directly connected to the corporate computer network and to the Internet via the standard RJ-45 cabling. By connecting it to the network, one can manage & monitor the unit via any standard web browser, such as Microsoft Internet Explorer & Mozilla Firefox.

The connection is very straightforward as shown in the following picture:

Make sure the computer has installed and has been configured with the TCP/IP Protocols.

iGuard can also be connected directly to the PC via crossover RJ-45 cable.

Note: Please contact iGuard Technical Support at (800) 441-6798 (US Only) or email to info@lucky.com.hk (international).

Power-up

During power up, iGuard will perform a self-test, then it will enter the standby mode as shown below: -

Description	***LCD Display***
1. Power Up – when iGuard is powering-up, it will perform a self-test…	`Initializing...`
2. After about 10 sec., the device will load the system program…	`iGuard Security` `Loading.....`
3. After loading the system program, iGuard will enter the Standby Mode and is now ready to set the date, time & the network settings.	`Thu Aug 30 12:00` `ID #:_ IN`

CONFIGURATION

Setting the date and time

The date and time must be properly set up so that iGuard can time stamp all the access & time attendance records. Follow these steps to set the system date and time: -

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Function Menu. You will be asked to enter the System Administrator Password.	`Enter Password:` `_`
2. Enter the System Administrator Password (default: 123).	`Enter Password:` `***_`

3. Press the **Func** key to continue. The function menu will scroll down slowly as shown.	`Press 1:`
	`Add/Update ID`
	⋮
	`Press 5: System`
	`Configuration...`

4. Enter **5** to select the **System Configuration** menu. The current date is displayed as shown. If necessary, enter the new date and then press the **Func** key to continue.	`Date (M/D/Y):` `08/30/2000`
5. After pressing the **Func** key, the current time is displayed. Enter the new time then press the **Func** key to continue.	`Time (H:M:S):` `13:24:43`

Description	***LCD Display***
6. The system will then ask for the Terminal ID, which is used to identify the iGuard in your network. The default ID is "iGuard". This ID is important especially if you have more than one unit installed.	**Terminal ID:** **_**

Note: iGuard can keep the date & time running without power for approximately one day. There is a software tool for users to synchronize the clock of the iGuard with the desktop PC (iSetClock.exe), which can be downloaded free of charge in the manufacturer's website.

Network Settings

To connect iGuard directly to your corporate network, a device name & an IP address are required. It is possible to use the DHCP server in the network to dynamically assign the IP address, but it is suggested that a static IP address be used.

The following procedures describe how to assign the name (i.e., the Terminal ID), the IP addresses, and other related network settings. Before proceeding the correct settings should already be obtained from the network administrator.

Description	***LCD Display***
1. *(…continue from step 6 above)* Enter the name of the device (e.g., A123). A more meaningful & descriptive name, such as "front door" or "sidedoor", can be assigned through the setup pages of the Web Interface (described in later sections).	**Terminal ID:** **A123_**
2. Press **Func** key to continue, and then press **2** to select "Static IP" instead of DHCP for now.	**DHCP/Static IP** **(1/2)? Static**
3. Press **Func** key to continue. You will then be asked to enter the IP address of the device. The default is 192.168.0.100. Change this default value if necessary.	**IP Address:** **192.168.000.100**
4. Press **Func** key, and then you will be asked to enter the port number. Use the default value 80 for now.	**Port Number:** **80_**
5. Press **Func** key to continue. Enter the subnet mask here (e.g., 255.255.255.0).	**Subnetmask:** **255.255.255.000**
6. Press **Func** key to continue. Enter the address of the Default Gateway (e.g., 192.168.0.200).	**DefaultGateway:** **192.168.000.200**
7. Press **Func** key to continue. Enter the address of the Domain Name Server (e.g., 203.80.96.15).	**DNS:** **203.080.096.015**

Description	***LCD Display***
8. Press **Func** key to continue. You will be asked if the device is a *Master* or *Slave* device. This is useful in a multi-device environment, where more than one iGuard are connected to each other. Refer to the section "*Master & Slave Mode*" for more detail.	**Master/Slave: (1/2)? Master**
9. Press **1** to select *Master* for now. When asked if you would accept the changes, press **1** to select **Yes**. The system may then reset itself and return to Standby Mode.	**OK to Accept Y/N (1/2)? Yes** ⋮ **Thu Aug 30 13:25 ID #:_ IN**

Warning: The IP address of the iGuard unit must be unique as in all other network devices. Otherwise, it will cause a network error and the iGuard will not function properly.

Note: The Terminal ID is NOT required to be unique, but a unique ID is recommended if multiple devices are installed in the same computer network, such as in a *Master / Slave* configuration.

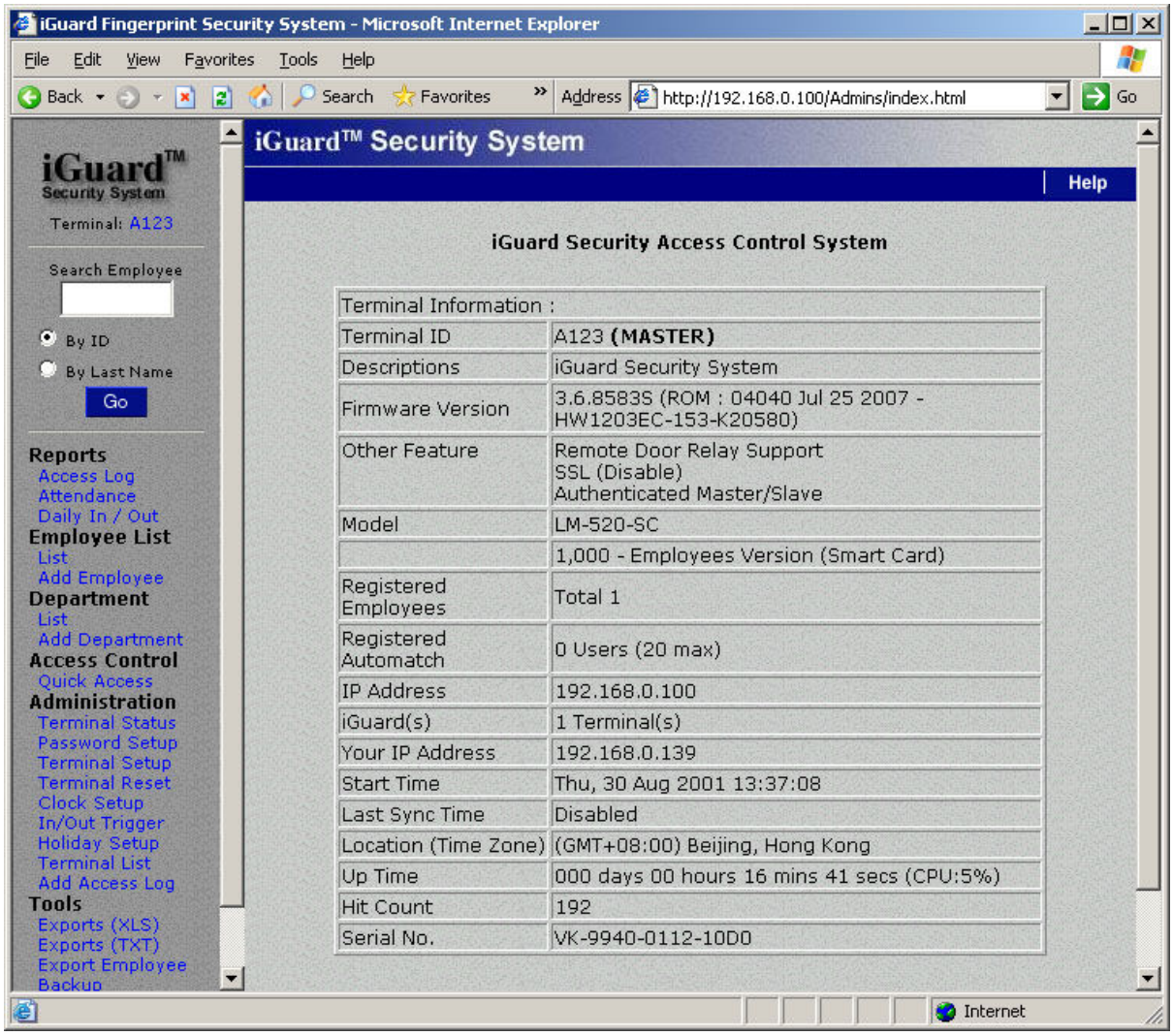
Verifying the Network Connections

One can test the above network settings by using a PC to *ping* the iGuard unit as follows:-

- Open the Command Prompt on the PC. To open Command Prompt, click **Start**, select **Run**, type **cmd**, and then click **OK**.
- Type **ipconfig** to check the IP address of the PC and make sure it is in the same network as iGuard (i.e., the same subnet mask).
- While still in the Command Prompt, use the **ping** command to ping the IP address of the iGuard unit as shown below, which is 192.168.0.100 in the above example.
- If the ping responds the following, the IP is set properly and the unit is ready.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=2ms TTL=128
Reply from 192.168.0.100: bytes=32 time=1ms TTL=128
Reply from 192.168.0.100: bytes=32 time=1ms TTL=128
Reply from 192.168.0.100: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Next, launch the PC web browser (e.g., Microsoft Internet Explorer), and enter the IP address **http://192.168.0.100** (i.e., the IP Address of the iGuard), and the following iGuard web interface will be shown in the browser window:-



At this stage, basic configuration is complete, and iGuard is now ready to use.

Note: All the system and network settings, as well as all the user data and access log, are saved in the non-volatile memory of the unit, and will be retained even if the power is off.

Getting Started

iGuard is a self contained, platform independent access control and time attendance solution. Most of the basic operations, such as user registration and verification, can be directly performed using the keypad of the unit itself without the computer and the web browser.

There are three methods for user authentication. These are the *Contactless Smartcard*, the *Fingerprint (optional)* and the *Personal Password*.

This section discusses the basic operations of these three approaches.

Adding and Verifying User with Smartcard

iGuard comes standard with built-in contactless smartcard reader. The System Administrator can use smartcard to create a new user, or to assign a smartcard to an existing user.

iGuard uses the standard Philips 1K Mifare Classic 13.56MHz Contactless Smartcard. It allows almost-instant verification for users, and it comes in handy when the device is used during the high-traffic period, for example, at the beginning of the day when everyone gets to the office at around the same time.

Adding New User with Smartcard

The following steps will show how to create a new user by issuing a new smartcard to the user:-

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Function Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **9** to select the item “Issue Smartcard”.	`Issue/Import Card (1/2)? _`
2. Enter **1** to select “Issue Card”. You will then be asked to enter the User ID.	`Enter ID # _`
3. Enter the user ID # (e.g. A01). The ID can be of any length from 1 to 10 characters, including the letters A & B.	`Enter ID # A01_`
4. If the ID does not exist, you will be asked to confirm to create this new ID.	`Create new ID... Yes/No (1/2)? _`
5. Press **1** to select Yes, then the unit will prompt you to present the Smartcard.	`Waiting for SmartCard...`

Description	***LCD Display***

6. Place a new Smartcard near the Keypad. Once the device has detected the Smartcard, it will update the card by writing the user information to the card.	`Writing...`
	⋮
	`Issue OK!`

7. Once it has finished updating the card, the unit will ask for the next user ID for issuing another Smartcard. Press **backspace** to return to Standby Mode.	`Thu Aug 30 13:28` `ID #:_ IN`

All the available user information, including the user name, personal password, access rights, and the fingerprint information (if any), will be written to the Smartcard memory.

Note: Only specifically-formatted iGuard Smartcard can be used with the device. Please contact the iGuard dealer or visit the manufacturer's website for more information about purchasing the Smartcard.

Verification with Smartcard

Verification with Smartcard is simple and straight forward, and is illustrated in the following steps:-

Description	***LCD Display***

1. While in Standby Mode, present the smart card near the keypad. The unit will read the data stored in the card. If the card is valid, the user will be authorized as indicated in the display. The unit will return to Standby Mode afterwards, and it is ready for the next card.	`A01`
	`Authorized!`
	⋮
	`Thu Aug 30 13:36`
	`ID #:_ IN`

Note: To achieve higher security level, iGuard can be configured to ask for the fingerprint image or *Personal Password* after presenting the smartcard for verification. It will be discussed in more detail in the next section under the heading "*Function 9: Issue / Import Card*".

Adding & Verifying user with Fingerprint (optional)

(This section is for iGuard with the optional fingerprint sensor only)

iGuard is optionally equipped with fingerprint sensor for fingerprint verification.

During the fingerprint enrollment process, the unit will ask for two fingerprint images for each person, and the information of the images is extracted and stored in the internal database for later verification. Each person must register two fingers: one as the primary and the other one as the secondary. Therefore, if the person's primary finger is

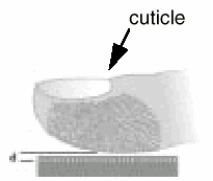
temporarily not suitable, such as when the finger is wounded, he can still use his secondary finger for verification.

During the process, each fingerprint image is captured three times for minutiae analysis and extraction. Minutiae are the mathematical representation of the fingerprint image. If the quality of any one of the three images is not good enough, the user will be asked to re-scan the three images again.

The two thumbs are suggested as the primary & secondary fingers. This is because the thumbs are usually bigger and can cover the scanner area better.

Hints for Capturing Fingerprint Images

Place the thumb flat on the fingerprint sensor using the pad, not the tip, of the thumb. The tip of the thumb contains the fewest minutia points, so place the thumb as flat as possible on the sensor to generate the fullest possible image.




The Core


The Tip

The core of the fingerprint containing the most minutia points is usually located opposite the cuticle. Center the cuticle in the sensor window to maximize the number of minutia points.

IMPORTANT: During the enrollment process, position the center of the fingerprint of the thumb to the center of the fingerprint sensor. The center of the fingerprint contains the most minutia points from which the fingerprint sensor can extract. *A good fingerprint image captured during the enrollment process can significantly reduce the false-reject rate during later verification.*

Adding New User with Fingerprint

The following steps will show how to register the user's fingerprint data:-

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Function Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **1** to select "*Add / Update ID*" menu.	`By Finger/Passwd (1/2)? _`
2. Press **1** to select "By Finger", then you will be asked to enter the user ID.	`Enter ID # and scan 1st Finger`
3. Enter the user ID # (e.g. A02). The ID can be of any length from 1 to 10 characters.	`Enter ID # and A02_`

Description	***LCD Display***

4. Press the **Func** key to confirm the ID #. The device now begins to capture the 1st image of the primary finger. The horizontal bar on the second line indicates the quality of the image. Lift the sensor shutter with your right-hand thumb and place it firmly on the sensor until the quality bar reaches the right end. You may need to move and rotate the thumb a little bit to achieve the required quality.	`Scanning 1 of 3`
	`|||||||`
	⋮
	`Scanning 1 of 3`
	`|||||||||||||||`

5. After the quality bar reaches the right end, you will be asked to remove the finger from the sensor.	`Analyzing. Pls` `Remove Finger...`
6. When the device detects that you have removed the finger, it will ask you to place it back again for the 2nd image of the same primary finger.	`Press Func to` `Scan 2 of 3`
7. Press the **Func** key and repeat the same procedure, and you will be asked to scan the 3rd time of the same primary finger.	`Press Func to` `Scan 3 of 3`
8. Press the **Func** key again and repeat the procedure for the third time. You will then be asked to scan the secondary finger.	`Press Func to` `Scan 2nd Finger`

9. Press the **Func** key, and repeat the above steps to scan the left-hand thumb three times again. If all the images are OK, you will see the acknowledge message momentary as shown, then the device is ready for the next enrollment.	`ID# A02`
	`Added OK!`
	⋮
	`Enter ID # and`
	`Scan 1st Finger`

10. Press the **Backspace** to return to the Standby mode.	`Thu Aug 30 13:34` `ID #:_ IN`

Note: If the user ID “A02” already exists, iGuard will prompt and ask if to overwrite the existing fingerprint information or not.

In case of poor fingerprint, for example, if the skin of a user is too dry or too wet, the user may experience difficulty when registering the fingerprint image, and the LCD display may show a message indicating a dry or wet fingerprint problem. Please refer to the *Fingerprint Enrollment* section in the Appendix for more information.

Verification

iGuard uses the enrolled fingerprint information to identify the person. The verification process is very straightforward, and is illustrated in the following steps: -

Description	***LCD Display***
1. While in Standby Mode, key in the user ID number (e.g., A02).	`Thu Aug 30 13:36` `A02_ IN`

2. Lift the shutter and place either your primary finger (right-hand thumb) or your secondary finger (left-hand thumb) on the sensor. You should place the finger the same way that you did during the enrollment procedure. The device will automatically start scanning after the sensor shutter has been lifted all the way up.	`Scanning...`
	`A02_`
	⋮
	`Verifying...`

3. If you are authenticated, the authorized message will be shown, and the unit will return to the Standby Mode.	`Authorized!`
	⋮
	`Thu Aug 30 13:36`
	`ID #:_ IN`

Note: There is another feature called *Auto-Match*, which allows the user to access the device without the need to enter his ID first. This feature will be discussed later in the "*Keypad Operation*" section.

Adding and Verifying user with Personal Password

In additional to Fingerprint and Smartcard, the user can also use the personal password for verification. The personal password is useful for the user who is not able to use fingerprint for verification (such as having skin problems), and does not want to use Smartcard.

Adding User with Personal Password

The following steps demonstrate how to add a new user with personal password:-

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Function Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **1** to select "**`Add/Update ID`**" menu.	`By Finger/Passwd` `(1/2)? _`
2. Press **2** to select "**`By Password`**", then you will be asked to enter the user ID.	`Enter ID #:` `_`
3. Enter the ID (e.g., A03).	`Enter ID #:` `A03_`

Description	***LCD Display***
4. Press the **Func** to confirm. Then enter the Personal Password for user A03. The password length can be up to 8 characters, including the characters A & B (e.g. 1234AB).	`User Password:` `******_`

5. Press **Func** to confirm. This new user has been added to the unit. The unit will then ask for the next ID to add.	`ID: A03`
	`Added OK!`
	⋮
	`Enter ID #:`
	`_`

6. Press **Backspace** to return to Standby Mode.	`Thu Aug 30 13:34` `ID #:_ IN`

Verification with Personal Password

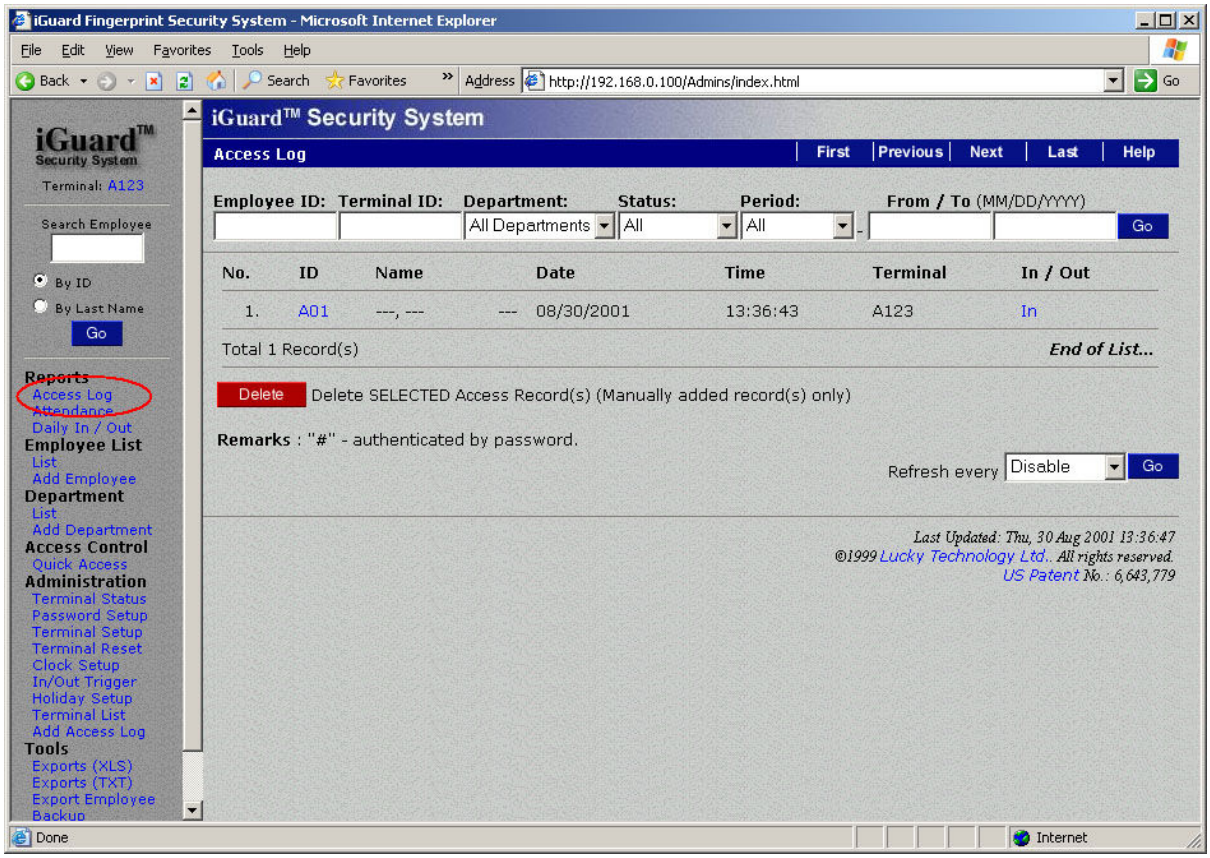
Once the personal password is assigned, the user can use it to get authenticated as follows:-

Description	***LCD Display***
1. While in Standby Mode, key in the user ID number (e.g., A03).	`Thu Aug 30 13:36` `A03_ IN`
2. Instead of using the fingerprint, press the **Func** key to indicate you are using the Personal Password. The unit will prompt you to enter the Personal Password.	`Your Password:` `_`
3. Enter the Personal Password (e.g., 1234AB).	`Your Password:` `******_`

4. Press the **Func** to confirm. If the password is correct, the unit will authorize the user, and will return to the Standby Mode as shown.	`A03`
	`Authorized!`
	⋮
	`Thu Aug 30 13:36`
	`ID #:_ IN`

Checking the Access Log

In the Web Browser, specify the IP address of the iGuard (e.g. http://192.168.0.100) to go to the iGuard webpage. Click on the Access Log link at the left side (circled in red), and the following entry in the access log will be shown:-



Note: Additional functionality is available through the keypad operation and web interface, which will be discussed in following chapters.

Master and Slave Mode

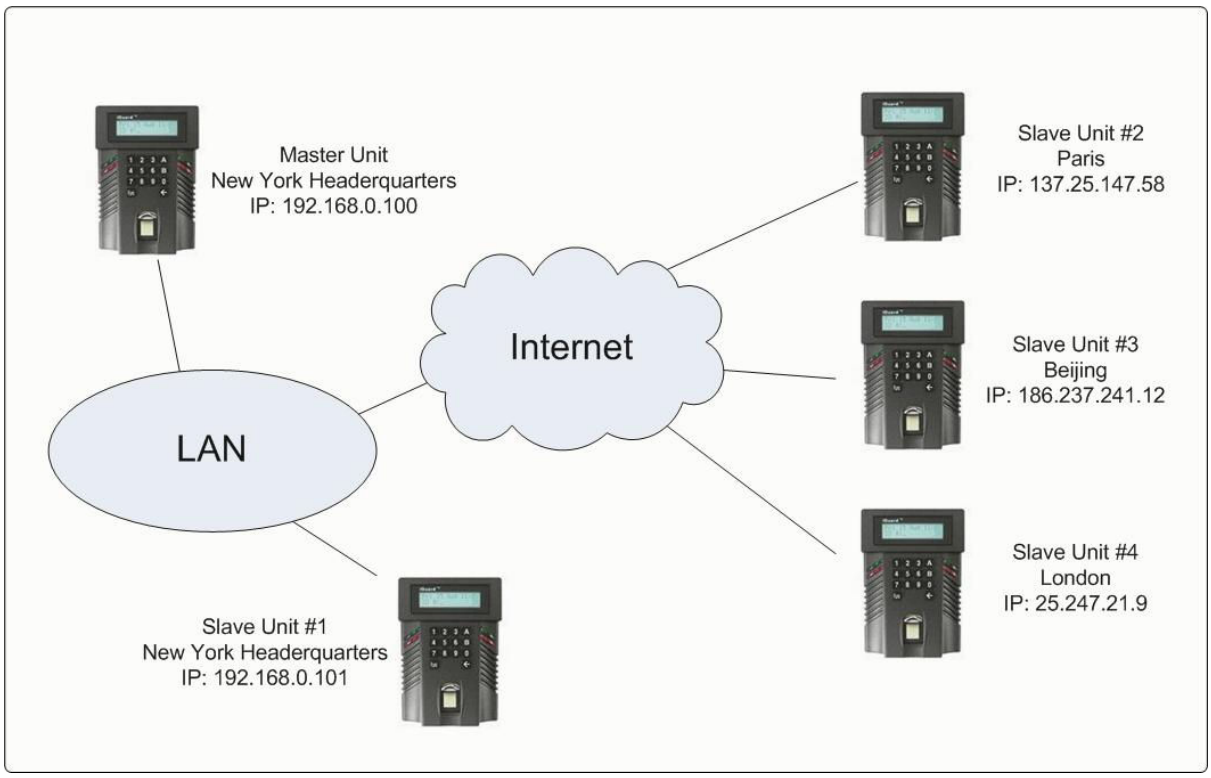
Each iGuard can be configured as a *Master* unit or a *Slave* unit.

By default, iGuard is configured as a Master unit. In a multi-device environment where more than one iGuard device is connected to the same corporate network or over the internet, these devices can form a Master / Slave network. In this case, one of these devices is assigned as the Master unit, and all others are assigned as Slave units.

The advantages of forming a Master / Slave network are:

- The system automatically replicates all the users' information to all devices in the master / slave network.
- Once a user registered in a unit (either a Master or a Slave unit), the information will automatically be replicated to all other devices, and the user can get access to and be verified by any one of the devices in the network.
- All access log records, such as the Clock-in and Clock-out records, created in any of these units are collectively saved in the Master unit, allowing the administrator to retrieve the access log records for all devices from a single location.
- Different access rights can be assigned to each individual iGuard unit.
- The master unit can optionally synchronize its clock with all the slave units (time zone adjusted).

The following is a typical Master / Slave setup:



In the above example, the Master unit is located in the New York Headquarters, and the other Slave units are installed in various places connected via the Internet. All the user information is replicated to all these units, and all the access log records of all these units are centrally saved in the Master unit.

Note: All units will still work even if the network connection is lost. And any new and modified user data or new access log records will be replicated automatically once the network connection is established again.

Basic Master / Slave configuration

The iGuard unit is configured as Master by default. Follow these steps to configure the unit as a Slave unit:-

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Function Menu. You will be prompted to enter the System Administrator Password as shown.	`Enter Password:` `_`
2. Enter the System Administrator Password (default: 123).	`Enter Password:` `***_`
3. Press the **Func** key to continue, and the function menu will appear.	`Press 1:` `Add/Update ID`
4. Enter **5** to select the **System Configuration** menu. The current date is displayed.	`Date (M/D/Y):` `08/30/2000`
5. Press the **Func** key 9 times to skip the other settings. You will then see the message asking if this unit is a master or slave unit.	`Master/Slave` `(1/2)? Master`
6. Enter **2** to select *Slave*. Then the unit will ask for the IP address of the Master unit.	`Master IP Addr:` `192.168.000.100`
7. Enter the IP address and press the **Func** key to continue. You will then be asked to enter the port number of the Master unit.	`Master Port:` `80_`
8. Enter the port number and press the **Func** key. The unit will reboot itself and then return to the Standby Mode.	`Thu Aug 30 13:25` `ID #:_ IN`
9. After a few seconds, if the Master unit can be reached, the user database will be synchronized from the master unit to this slave unit, and the corresponding message will appear during the process.	`Synchronizing,` `Please Wait...`
10. Once the synchronization is done, the unit will return to standby mode, and is ready for use.	`Thu Aug 30 13:28` `ID #:_ IN`

If the master unit is not reachable (e.g., the network connection is lost or the Master's IP address is wrong), the error message "*Master Offline!*" will appear on the LCD display.

Note: It is suggested that all units run on the same *firmware* version in a Master / Slave network. And one cannot mix the other iGuard model (e.g. the FPS model) with the LM model in a network.

Note: For security reason, the system administrator password of the slave unit must be the same as the Master unit. Otherwise, the master unit will reject the slave unit, and the error message "*Master Password Mismatch*" will appear. More on this topic will be discussed in the later section "*KEYPAD OPERATION → Function 0 → Configure Master / Slave"*.

KEYPAD OPERATION

This section will discuss the **Func** Key (i.e. the Function Menu) and the **Backspace** Key. More functions and options are available in the built-in web interface, which will be discussed in next section.

The Function menu

To enter the Function Menu, press the **Func** key in the Standby Mode and enter the System Administrator Password (default 123), then press the **Func** key again to confirm the password. Then the device will scroll and display all the available functions one by one.

There are 12 entries in the Function Menu, i.e., Function 0 to 9, A & B. They can be selected by pressing the corresponding key in the Function Menu.

The Function Menu	
Function 1 – Add / Update User	Function 7 – System Shutdown / Reset
Function 2 – Inactivate User	Function 8 – Set / Reset AutoMatch
Function 3 – Activate User	Function 9 – Issue / Import Smartcard
Function 4 – Delete User Fingerprint / ID	Function 0 – Advanced Feature
Function 5 – System Configuration	Function A – Toggle Test Mode
Function 6 – Set System Password	Function B – Open Door

Function 1: Add / Update User

This function is for adding a new user or updating an existing user by Fingerprint or Personal Password, as already discussed in the last section, *Getting Started*.

Function 2: Inactivate ID

A user ID can be temporarily suspended. This is useful if it is required to temporary remove a person's access to the facility, but might allow him to access again in the future. This is done via the function "Inactivate ID" in the function menu, and it is illustrated in the following steps:-

Description	***LCD Display***
1. While in the Function Menu, press **2** to select *"Inactivate ID"* menu.	`Enter ID #:` `_`
2. Enter the ID # you want to suspend (e.g., A01).	`Enter ID #:` `A01_`

Description	***LCD Display***

3. Press the **Func** key to confirm. The ID # is suspended, and the user can no longer be authenticated. Press **Backspace** to return to Standby mode.	`ID# A01`
	`Inactivated!`
	⋮
	`Thu Aug 30 13:44`
	`ID #:_ IN`

Function 3: Activate ID

This is to resume an Inactivated ID, and it follows the procedure similar to its counterpart function above.

Function 4: Delete Fingerprint / ID

Use this function to delete the fingerprint template of a user, or to permanently delete a user from the internal memory.

Follow these steps to delete the *fingerprint template* of the user:-

Description	***LCD Display***
1. While in the Function Menu, press **4** to select "`Delete Finger/ID`".	`Del Finger/ID` `(1/2)? _`
2. Enter **1** to select Finger. Then you will be asked to enter the user ID that the fingerprint template is to be deleted.	`ID to Del Finger` `A01_`

3. Press the **Func** key to confirm. The Fingerprint Template of the user is deleted, and he can no longer use his fingerprint to get authenticated. However, he can still use his Smartcard or Personal Password if available.
 	
Press **Backspace** to return to Standby mode.
	`ID# A01`
	`Finger Deleted!`
	⋮
	`Thu Aug 30 13:50`
	`ID #:_ IN`

Follow these steps to permanently delete a user from the internal memory:-

Description	***LCD Display***
1. While in the Function Menu, press **4** to select *"Delete Finger / ID"*.	`Del Finger/ID` `(1/2)? _`
2. Enter **2** to select ID. Then you will be asked to enter the user ID to delete.	`ID to Delete` `A01_`

Description	***LCD Display***

3. Press the **Func** key to confirm. The ID # is deleted, and the user can no longer access the system.
 	
Press **Backspace** to return to Standby mode.
	`ID# A01`
	`Deleted!`
	
	⋮
	
	`Thu Aug 30 13:47`
	`ID #:_ IN`

Note: Once the user ID is deleted, all the information associated with the user, including the fingerprint data, name, and the access right, will also be permanently deleted. The user must be re-registered to regain access rights. However, access log data will be retained.

Function 5: System Configuration

This is for setting up the system date and time, and for the network configuration, as discussed in the last section, *Getting Started*.

Function 6: Set Password

iGuard has three global passwords:-

- **System Administrator Password** – for system administrator to access the system menu and to configure the system. This password gives full access to the iGuard.
- **User Administrator Password** – for user administrator to manage the user accounts. Specifically, the user administrator can access the Function 1, 2, 3, 4 & 9 in the function menu only. This password does not give access to change system settings.
- **Door Access Password** – if *Quick Access* mode is enabled, users can use this password to bypass the normal user verification process to release the door strike. This *Quick Access* mode can only be enabled through the web interface, which will be discussed in more detail in the next chapter under the section "*Quick Access*" and "*Password Setup*".

Follow these steps to assign & edit these passwords:-

Description	***LCD Display***
1. While in Function Menu, press **6** to select *"Set Password…".*	`System Admin:` `***_`
2. Enter the new System Administrator Password (e.g., AB456). Note that you do not need to press backspace to erase the existing one.	`System Admin:` `*****_`
3. Press **Func** to confirm the new password. iGuard will then ask for the User Administrator Password.	`User Admin:` `_`

Description	***LCD Display***
4. Enter the new User Administrator Password and then press **Func** to confirm. Then you will be asked to enter the Door Access Password.	`Door Access:` `_`
5. Enter the new Door Access Password and then press **Func** to confirm. The unit will save the new passwords and return to the Standby Mode.	`Thu Aug 30 13:48` `ID #:_ IN`

Note: Both User Administrator Password & Door Access Password are optional. If it is not necessary to assign the password, just press the **Func** key without entering anything to skip the step. However, the System Administrator Password is not optional and must be assigned. The default is 123.

Note: The System Administrator Password of the Slave unit must be the same as the Master unit. Otherwise, the Master unit will reject the slave unit. In this case, an error message will be shown on the LCD display of the slave unit.

Function 7: Shutdown / Reset

Use this function to erase all the user and access log data stored in the internal memory, and to reset all the device settings to the factory default (such as setting the IP address to the default 192.168.0.100, and the terminal name to *iGuard* … etc.).

Follow these steps to reset and shut down the unit:-

Description	***LCD Display***
1. While in Function Menu, press **7** to select *"Shutdown / Reset"*. You will be asked whether to reset the User Database or not.	`Reset User DBase` `Yes/No (1/2)? _`
2. Press **2** to select NO, then you will be asked to reset the Access Log or not.	`Reset Access Log` `Yes/No (1/2)? _`
3. Press **2** to select NO, then you will be asked to reset all the settings to factory default or not.	`Factory Default` `Yes/No (1/2)? _`
4. Press **2** to select NO, then the unit will take a few seconds to prepare itself to shut down. Then it will show the message and it is now safe to power off the unit.	`It is now Safe` `To Power Off...`

Note: When the User Database or the Access Log are reset, all the data will be cleared when the unit is powered up again.

Note: If it is not necessary to reset the data, the device can be shut down safely by simply turning the power off.

Function 8: AutoMatch

Use this function to toggle the AutoMatch option between on and off for a user. AutoMatch enables the device to identify a person without requiring the user to first specify his user ID. This is also called 1-to-Many matching.

Following these steps to set the AutoMatch option for a user:-

Description	***LCD Display***
1. While in Function Menu, press **8** to select *"AutoMatch"*. You will be asked to enter the user ID.	**Enter ID #:** **_**
2. Enter the user ID (e.g., A01)	**Enter ID #:** **A01_**
3. Press **Func** to confirm. You will see the acknowledge message, and then the unit will return to Standby Mode.	**ID: A01** **AutoMatch Set!** ⋮ **Thu Aug 30 13:50** **ID #:_ IN**

After setting the AutoMatch option, the user no longer needs to enter his ID every time when accessing the device. The user can simply lift the shutter and place the finger on the sensor. The device will then automatically capture the image of the finger, and will try to match the captured image against the fingerprint information of ALL the AutoMatch-enabled users. The device will try to match the primary fingers first, and then the secondary fingers.

This feature can be assigned to any user; however, the maximum number of users is 30. This limitation is necessary for limiting the time the unit may take to match the image against all the AutoMatch-enabled users. It is therefore recommended that the AutoMatch feature is assigned to only the top management for convenience purpose. The rest of staff can use ID plus Fingerprint for access.

Also, users with poor fingerprint quality *should not* use AutoMatch because this option requires a higher quality of fingerprint image.

Follow the same procedure to toggle off this AutoMatch feature for the user.

Function 9: Issue / Import Smartcard

This function is for issuing the optional smartcard to new & existing users, and for importing existing smartcards to a new iGuard.

iGuard comes standard with a built-in contactless smartcard reader, which reads and writes user information to and from the smartcards. The information includes the user names, access right, fingerprint template, and personal password.

Please refer to the procedure on how to issue a Smartcard to new or existing users discussed in the section *Getting Started*.

Note: When issuing a smartcard to an existing user with fingerprint information, only the primary fingerprint is written to the smartcard. This is due to the limited smartcard memory.

There are three possible ways to authenticate a user using Smartcard. These are:

- Smartcard Alone
- Smartcard + Fingerprint
- Smartcard + Personal Password

The first method, *Smartcard Alone*, is already discussed in the chapter *Getting Started* earlier. It is applicable when the unit is in the *Quick Access* mode, or when there is no fingerprint or Personal Password assigned to the smartcard owner. In this method, all the user needs to do is to present the smartcard to the unit, and if the user has the access right to the unit, he will get authenticated instantly.

The *Quick Access* Mode is defined in the Web Interface, which will be discussed in the next chapter.

The 2nd method, *Smartcard + Fingerprint*, and the 3rd method, *Smartcard + Personal Password*, are used when the unit is not in the *Quick Access* Mode, and the user has previously enrolled his fingerprint or assigned his Personal Password.

Follow these steps to authenticate users using *Smartcard + Fingerprint* or *Smartcard + Personal Password*:

Description	***LCD Display***
1. While in Standby Mode, present the smart card near the keypad. The unit will read the data stored in the card. If the card is valid, the unit will ask for the Fingerprint Image or the Personal Password to continue…	`A02` `Waiting Finger/P`

scrolling message →	:
	`A02`
	`Password... Wait`

2. To authenticate using fingerprint, lift the shutter and place either your primary finger or your secondary finger on the sensor. To authenticate using Personal Password, simply enter the Personal Password and press **Func** to confirm.	`Scanning...`
	`|||||||`
	- or -
	`Your Password:`
	`****_`

3. If the Fingerprint or the Personal Password matches the record, the user will be authenticated, and the unit will return to the Standby Mode.	`A02`
	`Authorized!`
	:
	`Thu Aug 30 13:50`
	`ID #:_ IN`

This *Function 9* can also be used to import (register) an existing smartcard user to another iGuard unit.

This is useful if there are remote locations that are not tied into the master unit via a WAN of some kind, users of these remote locations can register to the master unit by importing their existing smartcards, rather than registering the fingerprint and other information to the unit once again, since all the information is already available in the smartcards.

Follow these steps to register an existing Smartcard user with the smartcard:-

Description	***LCD Display***
1. While in Function Menu, press **9** to select *"Issue / Import Card"*.	`Issue/Import Card (1/2)? _`
2. Press **2** to select *"Import Card"*, then you will be prompted to present the user's existing Smartcard.	`Waiting for SmartCard...`
3. If the Smartcard is valid, the information stored in the Smartcard, including the user name, fingerprint template, access right…etc, will be read and saved in the unit. The unit will then wait for the next Smartcard.	`ID: A02 Added OK!` ⋮ `Waiting for SmartCard...`
4. Press **Backspace** to return to the Standby Mode.	`Thu Aug 30 13:55 ID #:_ IN`

Please note that the administrator may still need to grant the user's access rights by assigning the departments the user belongs to.

Note: "Department" is used for assigning access rights to different users at different time & terminals. Please refer to the section "Department" in the next chapter, *Using The Web Browser*, for more information.

Function 0: Advanced Feature

This function contains a number of handy tools for setup and network diagnosis.

1. Connection Test

This is for testing the network connection between two iGuards. It shows the connection speed with the target iGuard. It also shows the Firmware Version and the Serial Number of the target unit, as shown in the following example:

Description	***LCD Display***
1. While in Function Menu, press **0** to select *"Advanced Feature"*. Then you will be asked if you want to perform a *Connection Test*.	`Connection Test Yes/No (1/2)? _`

Description	***LCD Display***
2. Press **1** to select *Yes*, then you will be asked to enter the IP address of the target iGuard. Enter the IP address of the target iGuard.	`IP Address:` `192.168.000.123_`
3. Press **Func** to confirm, and then enter the Port number.	`Port:` `80_`

4. Press **Func** to confirm. If the target iGuard is valid, the Firmware Version, the connection speed, and the target Serial Number of the target iGuard will be displayed as shown.
 	
(note: only the last 8 digits of the serial number are shown)
	`Target Firmware`
	`Ver: 3.6.8583`
	⋮
	`Echo Received`
	`Time: 190ms`
	⋮
	`Target Serial`
	`No: 021A-121F`

5. Press **Backspace** to return to the Standby Mode.	`Thu Aug 30 13:56` `ID #:_ IN`

This test is only for testing the connection between Master and Slave units.

2. Ping Test

This test is analogous to the same test in PC. It is different from the Connection Test in that it works with any network device, not just iGuard. It comes in handy when it is necessary to test the connection between the iGuard and a PC, for example.

Description	***LCD Display***
1. While in Function Menu, press **0** to select *"Advanced Feature"*. Then you will be asked if you want to perform a *Connection Test*.	`Connection Test` `Yes/No (1/2)? _`
2. Press **2** to select NO to skip the *Connection Test*, then you will be asked if you want to perform a *Ping Test*.	`Ping Test` `Yes/No (1/2)? _`
3. Press **1** to select YES, then you will be asked to enter the IP address of the target device. Enter the IP address of the target device.	`IP Address:` `192.168.000.123_`

4. Press **Func** to confirm. The unit will try to ping the target device, and display the result as shown.	`192.168.000.123`
	`Ping:#1 5ms`
	⋮
	`192.168.000.123`
	`Ping:#3 7ms`

Description	***LCD Display***
5. Press **Backspace** to return to the Standby Mode.	`Thu Aug 30 13:57` `ID #:_ IN`

3. Configure iServer (for Master Mode only)

This is for configuring the iGuard to work with the iServer.exe, which is a Windows-based program that runs on PC, to allow using the PC to store all the Access Log permanently.

The program, iServer.exe, can be downloaded free of charge in the manufacturer's website.

Please refer to the Appendix for more information about this iServer.exe program.

4. Configure Master/Slave Password Authentication (for Master Mode only)

A new feature has been introduced in this firmware release that enables the Master unit to check against the Slave unit's *System Administrator Password*, and only accepts the slave units that match the password with the Master unit. As a result, only authorized Slave units can be connected to and communicate with the Master unit.

If the slave unit's *System Administrator Password* does not match with the one in the Master unit, the Slave unit will be rejected, and an error message will be shown on the LCD display of the Slave unit.

However, this feature is not available in previous firmware release, and the Master unit by default will not check the password for the Slave unit that runs on the previous firmware versions. Therefore, for security reasons, the Master unit may be configured so that it will not accept any slave unit that runs on the old firmware version, as illustrated in the following:-

Description	***LCD Display***

1. While in Function Menu, press **0** to select *"Advanced Feature"*, then press **2** a few times to skip the other items until you get to the item "*Configure Master / Slave Password Authentication*".
scrolling message →
	`Configure Master`
	`Yes/No (1/2)? _`
	⋮
	`Authentication..`
	`Yes/No (1/2)? _`

2. Press **2** to select YES for this "*Configure Master / Slave Password Authentication*" item. Then you will be asked if you want to disable the slave units that run on old firmware release.
scrolling message →
	`Disable for Slav`
	`Yes/No (1/2)? _`
	⋮
	`than 3.6.8583?..`
	`Yes/No (1/2)? _`

3. Press **1** to select YES. This Master unit will now reject any slave unit that runs on firmware version earlier than 3.6.8583. The unit will then return to Standby Mode.	`Thu Aug 30 13:59` `ID #:_ IN`

5. Trigger Alarm When Unauthorized

This option allows the iGuard unit to turn on the Alarm for all unauthorized access. This includes the unauthorized access such as *Invalid ID*, *No Access Right*, *ID Suspended* … etc. When enabled, if an unauthorized access occurred, the terminals #10 & #11 at the back of the unit will close the circuit for approximately five seconds. If an alarm is properly connected to these two terminals, the alarm will sound.

Follow these steps to enable this option:

Description	***LCD Display***
1. While in Function Menu, press **0** to select *"Advanced Feature"*, then press **2** two times to skip the other items until you get to the item "*Trigger Alarm When Unauthorized*".	`Trigger Alarm Wh` `Yes/No (1/2)? _`

scrolling message →	:
	`Unauthorized...`
	`Yes/No (1/2)? _`

2. Press **1** to select YES to turn on the option. Now the iGuard will close the terminals #10 & #11 at the back for approximately 5 seconds when there is unauthorized access. The unit will then return to the Standby Mode.	`Thu Aug 30 14:02` `ID #:_ IN`

6. Set Quick Enroll (for units equipped with Fingerprint Sensor only)

Reserved for backward compatibility. Do not enable this option.

7. Reset User In/Out Status (for Master Mode only)

iGuard keeps a list of all users' IN/OUT status and the corresponding date & time information. This can be viewed on the "*Employee List*" webpage (which will be discussed in the next chapter). This option is to clear the information.

Follow these steps to reset the User In/Out Status:

Description	***LCD Display***
1. While in Function Menu, press **0** to select *"Advanced Feature"*, then press **2** four times to skip the other items until you get to the item "*Reset User In / Out Status…*".	`Reset User In/Ou` `Yes/No (1/2)? _`

scrolling message →	:
	`In/Out Status...`
	`Yes/No (1/2)? _`

2. Press **1** to select YES to reset the user status. Now the iGuard will clear all the existing users' In / Out status. The unit will then return to the Standby Mode.	`Thu Aug 30 14:08` `ID #:_ IN`

Note: By default, the User Status information is automatically reset daily at 12:00am. This

is user definable in the webpage discussed in next chapter.

8. Pack & Re-Index Database

This is to re-index and compact both the user database and the access log saved in the internal Flash Memory.

Normally, it is not necessary to perform this function, since the iGuard is designed to periodically perform the function in the background automatically without user interference. However, in the very unlikely event, should there be something wrong with the Database (e.g., some of the existing users or some of the access log entries are missing), follow these steps to re-index the databases:

Description	***LCD Display***
1. While in Function Menu, press **0** to select *"Advanced Feature"*, then press **2** a few times to skip the other items until you get to the item "*Pack Database*".	`Pack DBase` `Yes/No (1/2)? _`

2. Press **1** to select YES to re-index and compact the Databases. iGuard will first re-index and compact the user database, followed by the access log database. After the operation has completed, the unit will return to Standby Mode.	`Packing Users`
	`|||||||`
	⋮
	`Packing Log`
	`|||||||||||`
	⋮
	`Thu Aug 30 14:15`
	`ID #:_ IN`

Function A: Test Mode Toggle

By default, iGuard records all the user access in the Access Log. The device can be set to the ***Test Mode***, and it will temporarily stop recording the transactions. This feature comes in handy when, for example, someone wants to "practice" with or test the device by clocking in and out with the fingerprint, but does not want to include these records in the access log.

Follow these steps to toggle the test mode:-

Description	***LCD Display***
1. While in Function Menu, press **A** to toggle the device to Test Mode. The unit will return to Standby Mode, and the "*Test Mode*" status will appear on the 1st line as shown.	`Test Mode!` `ID #:_ IN`
2. Repeat the above step and the unit will return to the normal Standby mode.	`Thu Aug 30 14:15` `ID #:_ IN`

Note: The *"Test Mode"* must be toggled back to *"Normal Mode"* before the unit will begin to record transactions in the access log again.

Function B: Open Door

This is for the System Administrator to quickly open the door without going through all the verification procedure.

This feature has been added as a backup mean to open the door. In the unlikely event when the iGuard fails to read any smartcard or fingerprint image due to hardware failure, the System Administrator can still have a way to open the door.

Description	***LCD Display***

1. While in Function Menu, press **B** to open the door. The door will then open and unit will return to the Standby Mode.	`Open Door!`
	⋮
	`Thu Aug 30 14:17`
	`ID #:_ IN`

The Backspace Key

The backspace key on the keypad mainly serves three functions: to erase the last entered key, to abort in the middle of an operation, and to toggle the access status between IN and OUT during Standby Mode. This section will discuss how to use the Backspace key to toggle the access status.

The default access status is IN, as shown in the 2nd line of the LCD display when the unit is in Standby Mode. Follow the steps below to change the access status from the default IN to OUT:-

Description	***LCD Display***
1. In Standby Mode, the default access status is shown in the 2nd line of the display (which is IN in this case).	`Thu Aug 30 16:36` `ID #:_ IN`
2. Press the **Backspace** key and the access status will be changed to OUT. Then follow the usual procedure to continue (e.g. enter the user ID and present the smartcard).	`Thu Aug 30 16:36` `ID #:_ OUT`

3. If no key is pressed for approximately 5 seconds, the unit will show the *Time Out* message, and will return to the default access status.	`Time Out!`
	⋮
	`Thu Aug 30 16:36`
	`ID #:_ OUT`

Note: The default access status can be set to either IN or OUT in the *"In / Out Trigger"* page via the web browser.

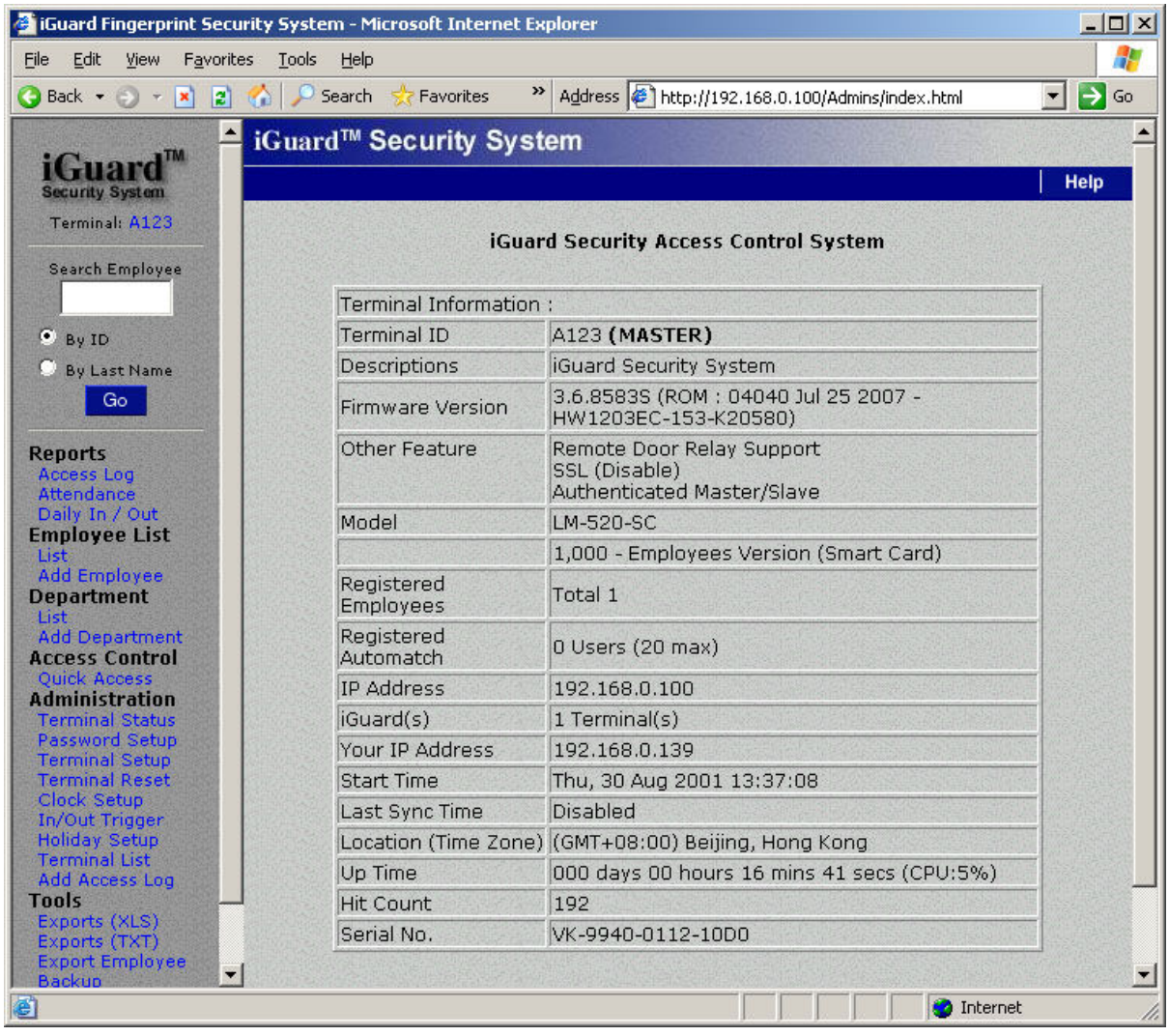
USING THE WEB BROWSER

iGuard has a built-in web server which operates exactly like a hosted web site. The web interface gives the system administrator a simple, easy to use set of tools to configure and maintain the unit and the users. Retrieve the access log records and other data with any standard web browser, such as Microsoft Internet Explorer or Mozilla Firefox.

With this feature, the unit may be accessed by any PC connected to the corporate network, without the need for any dedicated PC or any special software package. If the iGuard is connected to the Internet, it can even be accessed from anywhere in the world via the Internet.

iGuard is platform independent. It can be a Windows-based machine running Microsoft Windows Vista, a Linux machine or an Apple iMac machine, as long as it runs the standard web browser.

Once connected to the corporate computer network, the unit may be accessed by specifying the IP address in the Web Browser (e.g., http://192.168.0.100). This is the IP address assigned to the iGuard during the setup procedure previously discussed. The following will appear in the browser: -



The above iGuard's home page is divided into left & right panels. Select different items in the left panel and the right panel will display the corresponding pages.

This chapter will discuss each of these items in detail.

Reports

There are three types of reports: *Access Log*, *Attendance*, and *Daily In/Out*.

Access Log

Click on the link **Access Log** in the left panel and something similar to the following will appear: -

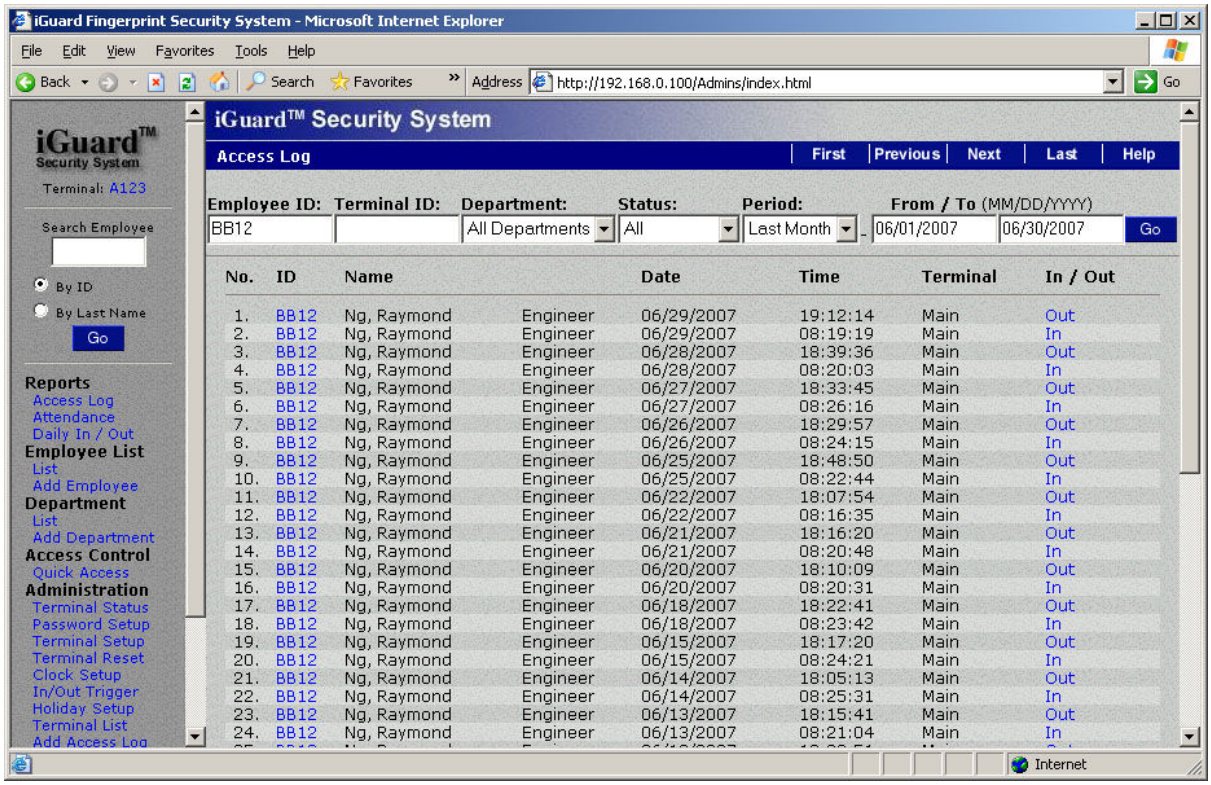
This page shows the employees' Access Log. iGuard keeps the most recent 10,000 access log records in the internal memory based on the First-IN-First-OUT rule. When the number of access log records exceeds 10,000, iGuard will delete the oldest record automatically to make room for the new one.

To show the records of a particular person only (e.g., BB12), enter his ID # in the *Employee ID* text box and press the **Go** button, and only the records of this person will be shown. Specify the *Department*, and only the particular department members will be shown.

The *Time Period* may be specified such as displaying only *today's* records, *last week* records, *last month* records… etc., or specify the Time Period by choosing the *Range* selection and entering directly to the From / To fields.

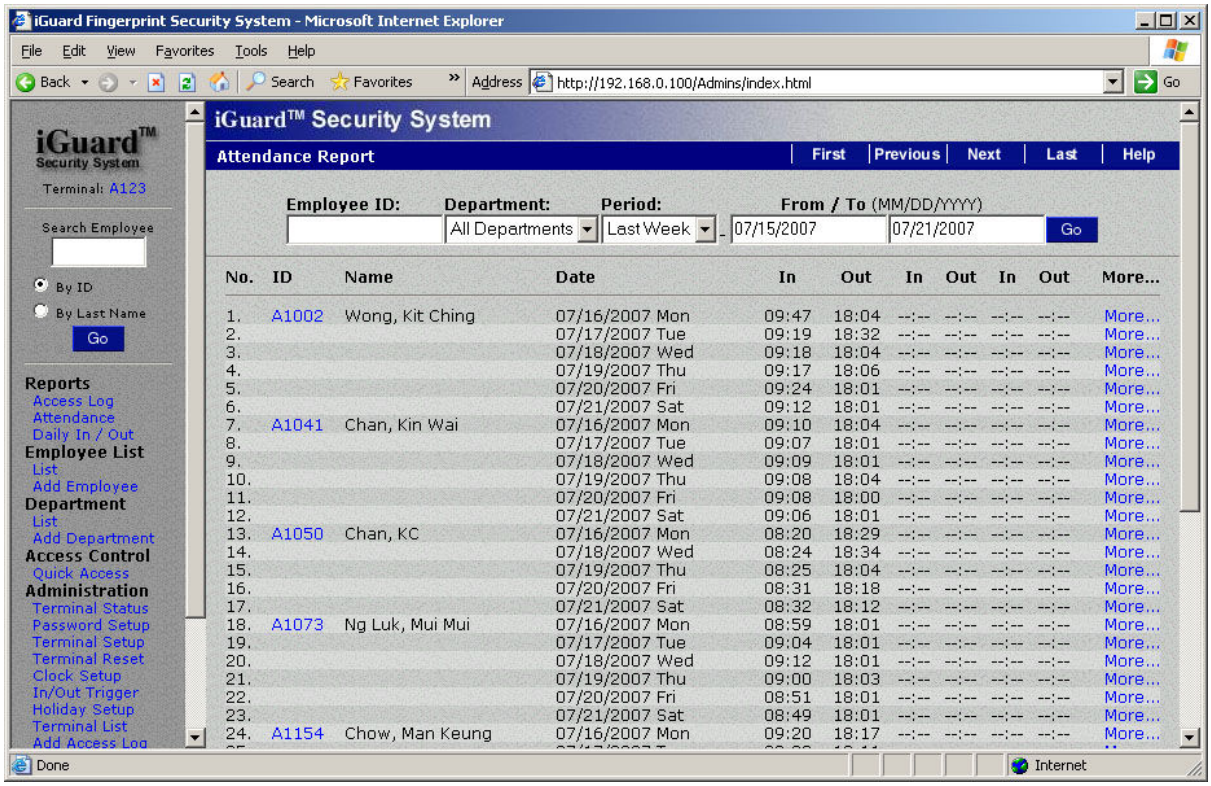
Press the **Next** button in the navigator bar at the top of the page to move on to the next page, or jump to any particular page by clicking on the page number at the bottom.

The following example shows only the *Last Month* records of the employee ID # BB12: -



Attendance

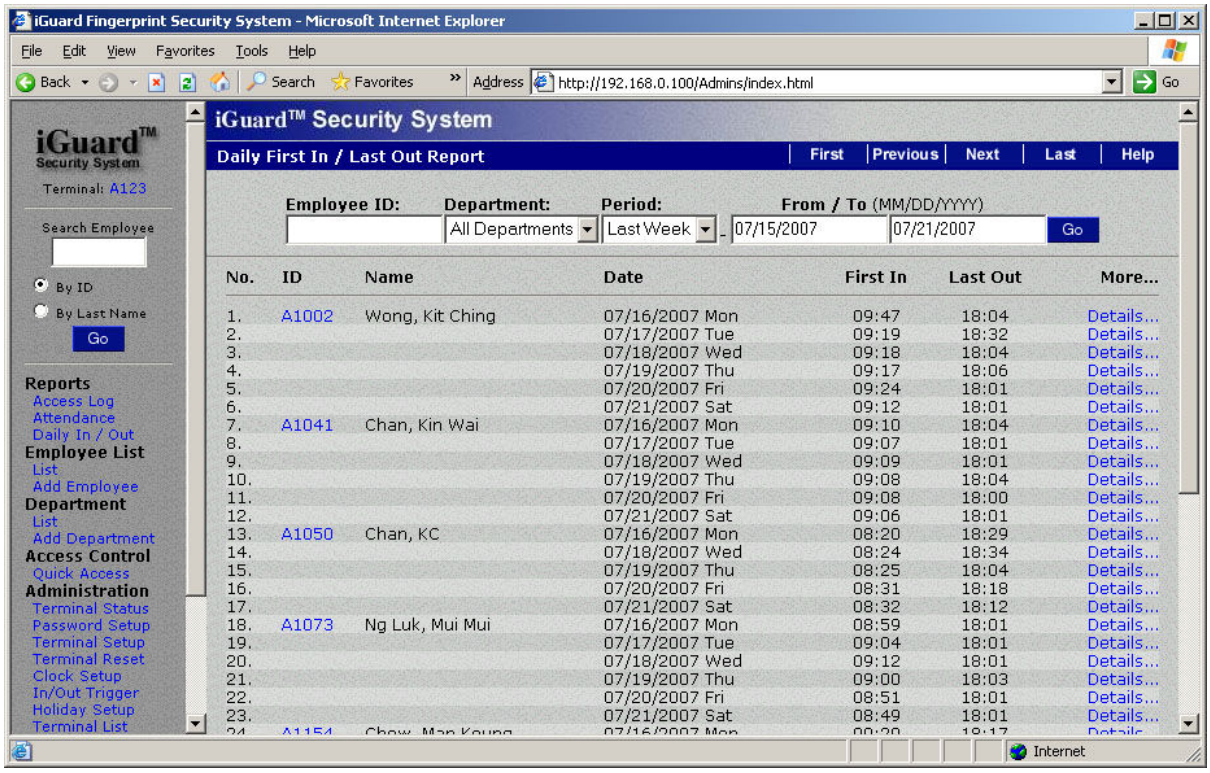
The attendance reports provide a consolidated access records of each person as follows:-



The Attendance Report is particularly useful for payroll purpose. And similar to the Access Log Report above, the employee's ID and / or the Time Period of the Attendance Report can be specified.

Daily In / Out

The Daily In / Out Report is very much the same as the Attendance Report discussed above, except that it only shows the first IN time and the last OUT time for the day as shown below:-



Employee List

The maximum number of registered users is 1,000, and they are shown in the Employee List page. Each individual user may also be managed in this page using the browser.

The *System Administrator Password* is required for these operations. The Web Browser will prompt for the *User Name* and *Password* when accessing the employee functions. The default *User Name* is *"admin"*, and the default *Password* is *"123"*, as shown in the figure below:-

List

The *Employee List* shows all the registered employees as shown below:-

There are four columns on the right side of the list with *green* or *grey* (i.e., ON / OFF) indicators. These are: -

- The ***Active*** Indicator indicates that the employee is in Active status (i.e., not suspended).
- The ***FP*** (Fingerprint) indicator shows whether the user has registered his fingerprint image, and he can use fingerprint for authentication.
- The ***SC*** (Smartcard) indicator shows that a Smartcard has been issued to the user.

- The ***PSW*** (Password) indicator shows a Personal Password has been assigned to the user. Personal Password is optionally assigned to each individual user using **Func 1** in the function menu as discussed previously, or can be assigned using the browser in the user setup page, which will be discussed later in this section.

- The ***AM*** (Auto-Match) indicator indicates that the optional auto-match feature is enabled for the particular user. If enabled, during fingerprint authentication, the user can simply lift the shutter and place the finger on the sensor for authentication without the need to enter his ID first.

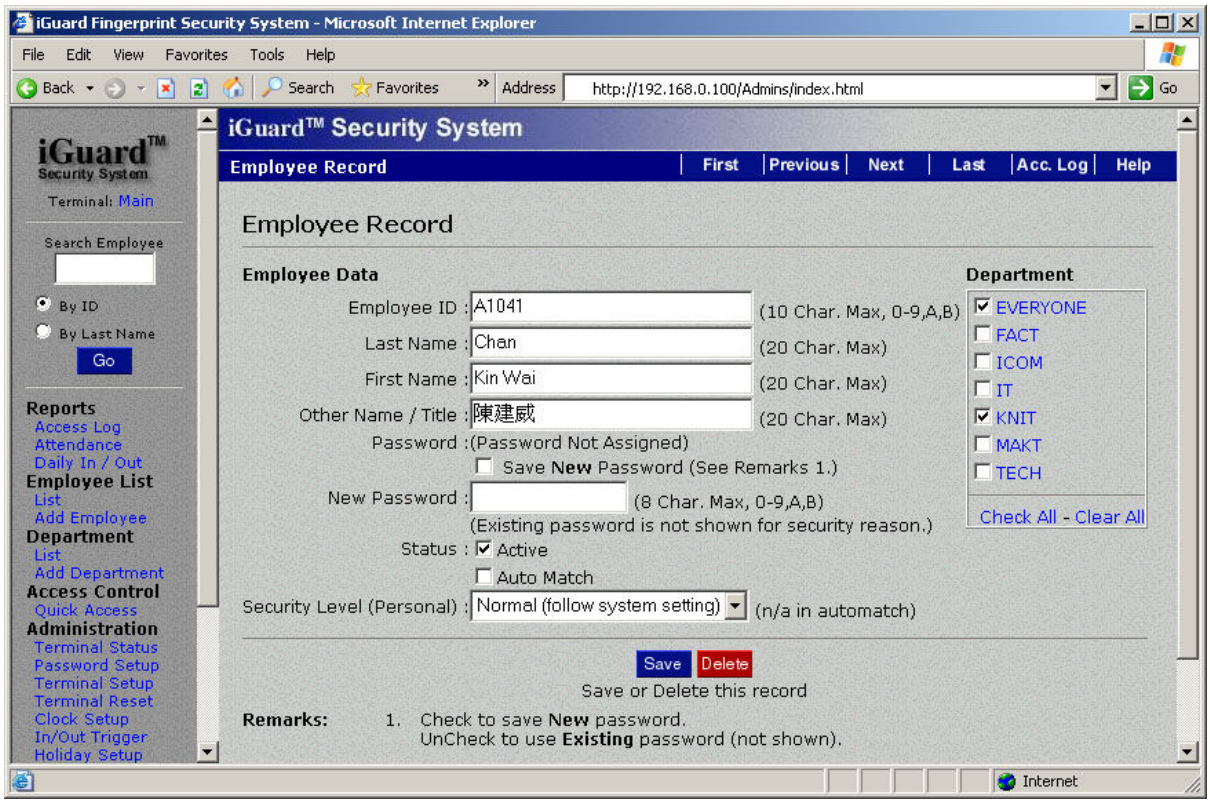
The last column is the *In/Out monitor* for each employee, which shows the time and the access status of the corresponding last access entry. The information is reset daily at midnight by default, and this default time can be changed in the *Terminal Setup* page of the web interface.

The text boxes at the top allow you to search and filter these results by First Name, Last Name, Status and Department.

Scroll down to the bottom of the right panel, and the three buttons, Activate, Deactivate & Delete, will appear. One can Activate, Deactivate & Delete a single employee or a group of employees by first checking the checkbox and then pressing the corresponding button.

Note: Once the user ID is deleted, all the information associated with the user, including the fingerprint data, name, and the access right, will also be permanently deleted. The user must be re-registered to regain access rights. However, access log data will be retained.

Press the employee ID hyperlink to edit the information of each employee, as shown in the following figure:-



Use this page to edit the employee information in this page.

Employee ID – The ID is a unique value, up to 10 characters, and is limited to the characters 0-9, A, and B. This is because these are the only characters on the keypad of the iGuard unit.

Last Name, *First Name* & *Other Name / Title* – Enter the name and the title of the user.

Password – Enter the Personal Password of the user.

Active – The default user status is *Active*. Uncheck this box if it is necessary to temporarily suspend the user's access rights.

AutoMatch – Check this option to include this user in the AutoMatch group for the 1-to-many fingerprint matching.

Security Level (Personal) – This is for the unit with the optional fingerprint sensor only. Select the default "*Normal (follow system setting)"*, and the fingerprint matching security level of this user would follow the system security level. Select other security level (such as Low) for users with difficulty in fingerprint matching, such as those with skin problems.

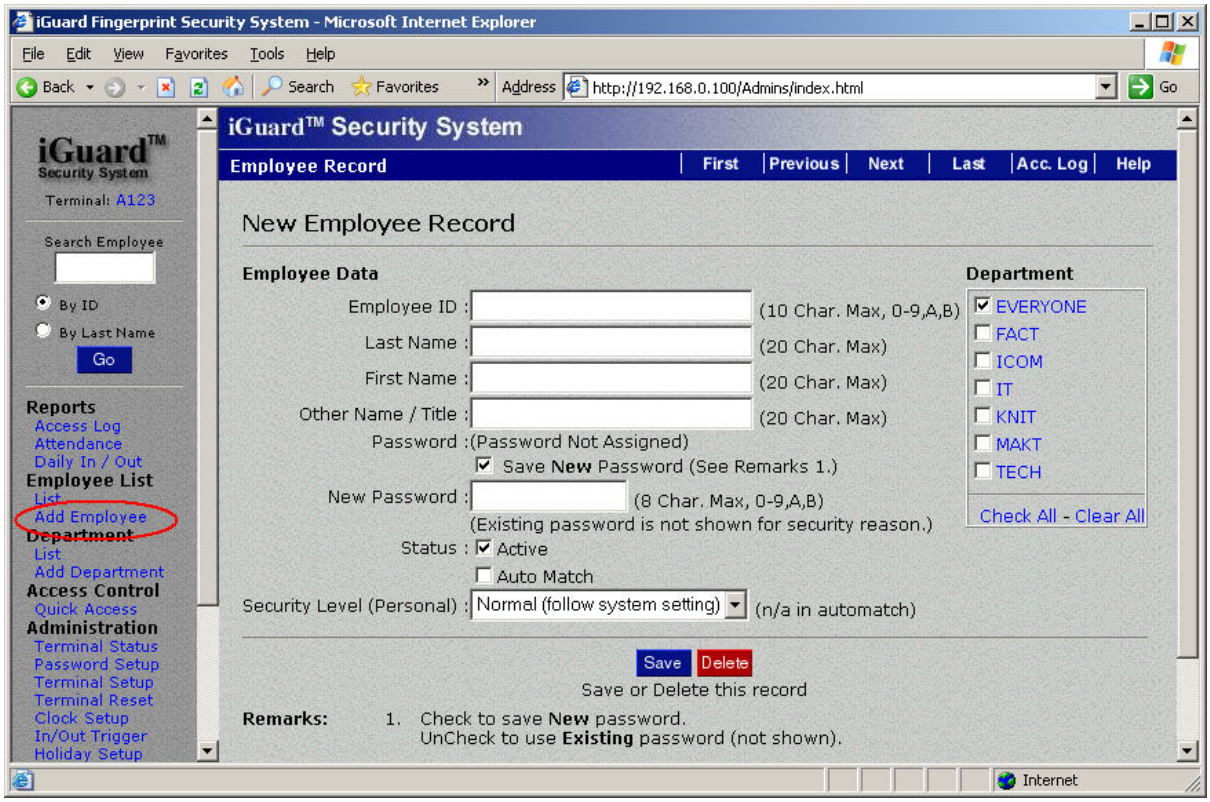
Department – This is to assign the user to different departments by checking the checkboxes in the department list on the right side of this page. The default department is EVERYONE. More details about the Department will be discussed in the next section.

Press the **Save** button at the bottom to save the change.

Press the **Delete** button to delete this particular employee,

Add Employee

In addition to adding new users to the unit using the keypad procedure discussed in the "Getting Started" section earlier, users may also be added from the *"Add Employee"* page, as shown in the following figure:-



By default, the department EVERYONE is assigned to all new users. Uncheck the checkbox if no department is to be assigned to the user.

After adding the user, follow the same procedure discussed above to further assign a smartcard to the user (i.e., using the **Func 9** menu) if the user is to use smartcard for authentication. Similarly, for iGuards equipped with the optional fingerprint sensor, the user needs to register his fingerprint using the **Func 1** menu discussed above for fingerprint authentication.

Department

Prior to adding employees to the iGuard unit, it is a good idea to establish departments. For smaller companies, this may not be as applicable, but departments are helpful for establishing permission to individual iGuard units, and access times for groups of employees.

In a typical setting, the Executive and Accounting departments may be the only employees with access to the accounting file room during normal business hours, and your Tech department might contain anyone authorized to enter the server room at any time, while everyone in the company can come and go through the front door at any time except weekends and company holidays.

The system default department is "*EVERYONE*" and it cannot be deleted. By default, each new employee created will automatically be added to the "*EVERYONE*" department.

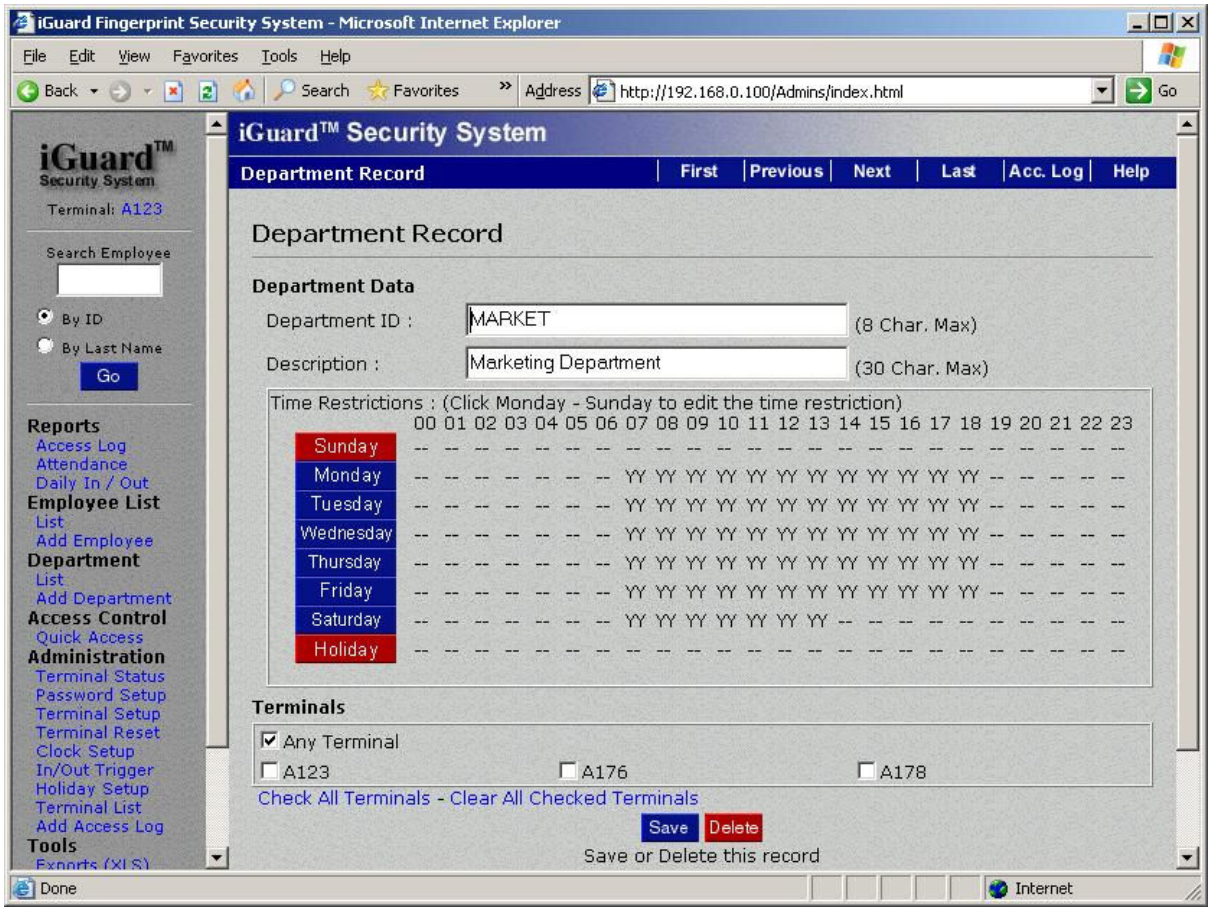
A maximum of 32 departments is allowed in the unit, including the default department "*EVERYONE*". The maximum length of the Department ID is 8 characters.

Department List

This page shows all the departments currently assigned to the system:

To delete a single department or a group of departments, first check the checkboxes of the departments, and press the **Delete** button at the bottom. Please note that the default department, EVERYONE, cannot be deleted, and it does not have a corresponding checkbox next to it.

Click on the Department ID hyperlink to edit the access right for each individual department. For example, to edit the marketing department, click on the Department ID *MARKET*, and the following page will appear:-

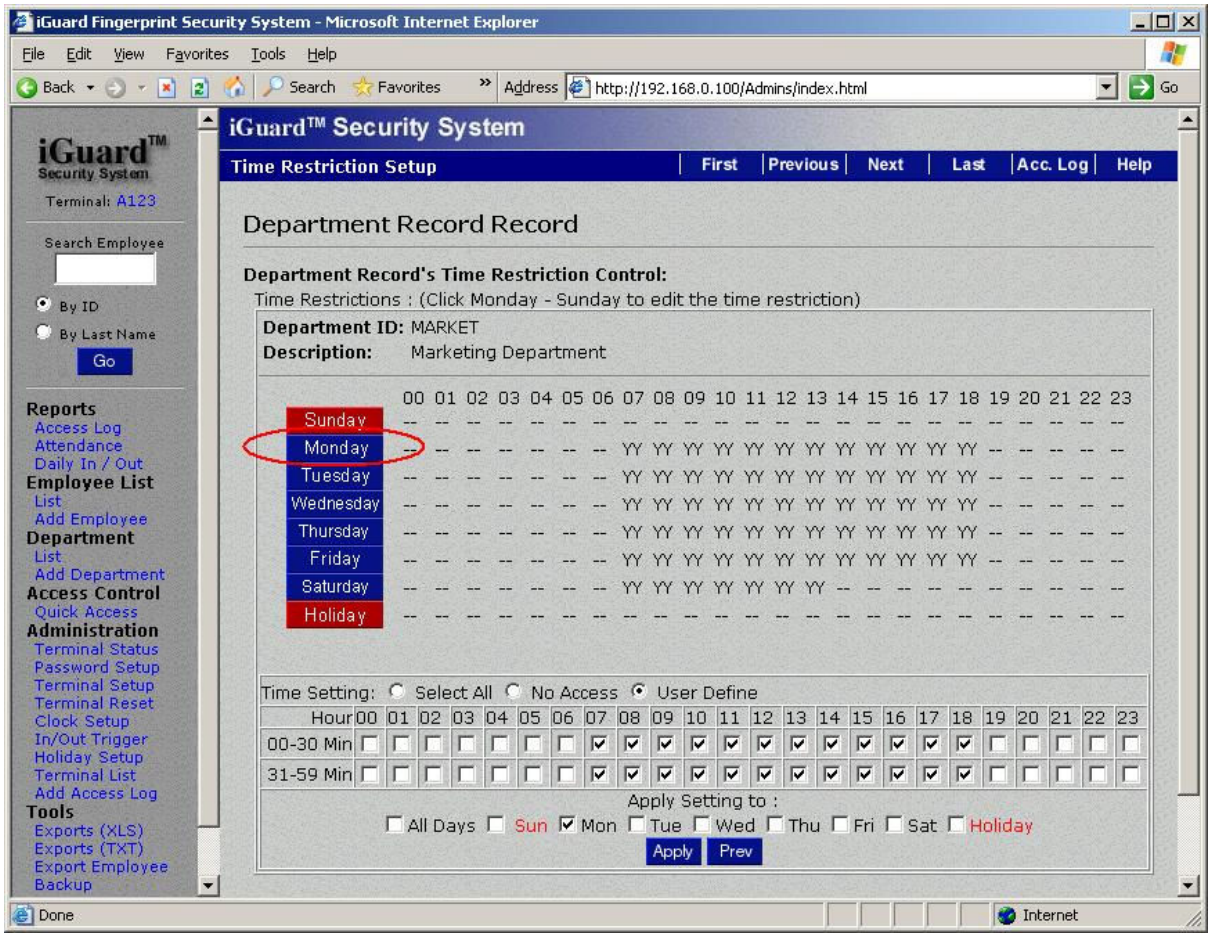


The above page indicates that the authorized time period for the *Marketing Department* is from 7:00am am to 6:59 pm, Monday to Friday, and from 7:00am to 13:59pm on Saturday. All the members of this department can only access the unit during this authorized period.

The bottom part of the page, *Terminals*, specifies the “doors” to which this department has the access rights. This is only applicable when multiple iGuards are connected together and form a Master / Slave network. If there is only one iGuard or the iGuard is not connected to any Master / Slave network, there will only be one item in this “*Terminals*” section, which is the Terminal ID of the iGuard itself.

Check the checkbox “*Any Terminal*” to allow the department members to access any iGuard unit in the network.

The authorized time of a particular day, Monday for example, can be edited by clicking on the *Monday* button, and the following web page will appear.



The authorized time period can be selected at the bottom of the page. If it is necessary to select all the time slots, simply select the "*Select All*" checkbox above. The "*All Days*" checkbox can also be selected to include all the days of the week.

The *Holiday* option is set in the *Holiday Setup* page, which will be discussed later in this chapter.

Add Department

Use this page to add new department. The operation is similar to the steps discussed above.

Note: The maximum number of departments is 32, including the default department *EVERYONE*.

Access Control

Quick Access is an access control feature of iGuard which, when activated, allows users to come and go without authenticating individually. The system administrator can authorize this *Quick Access* period by specifying the time, dates and the terminals.

There are three ways to utilize this feature:-

- *Quick Access Password* – This password can be given to Emergency Medical Services, building maintenance, or your mail carrier. This can be useful if it is

necessary to keep the facility locked but without the need to record the individuals who are coming and going during business hours.

- *Smartcards* – For users with smartcards, this *Quick Access* will let them enter and exit with the smartcard, and will not ask for fingerprint or personal password.

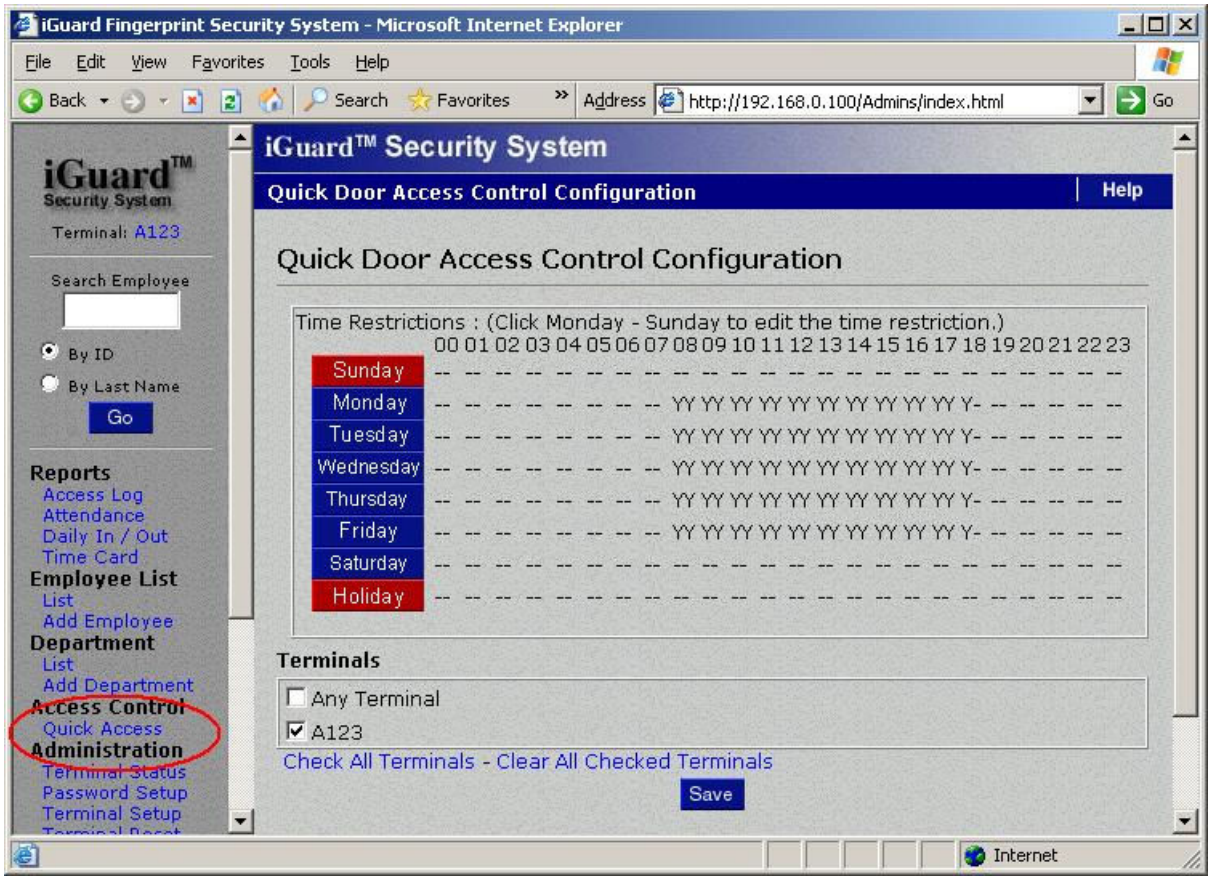
- *Quick Access By Key-In ID* – If this option is enabled, the user can perform this *Quick Access* function by simply entering his user ID. This option is found in the webpage under "*Terminal Setup → Others Options → Quick Access By Key-In ID*", which will be discussed in later section.

In a typical setting, one can enable this *Quick Access* period during the normal office hour when the traffic is high and the security requirement is low, and disable the *Quick Access* otherwise. In this setting, users only need to present their Smartcards to get authenticated to speed up the authentication process. But they need to use both Smartcards and Fingerprint or Personal Password during the other time that requires higher security level.

This section will illustrate how to configure this *Quick Access* period.

Quick Access

Use this page to define the authorized *Quick Access* period and the corresponding iGuard units. The default setting is NONE, i.e., there are no authorized terminals or access times for *Quick Access*.



The procedure for setting the valid period for Quick Access is similar to the procedure for setting up the departments discussed above.

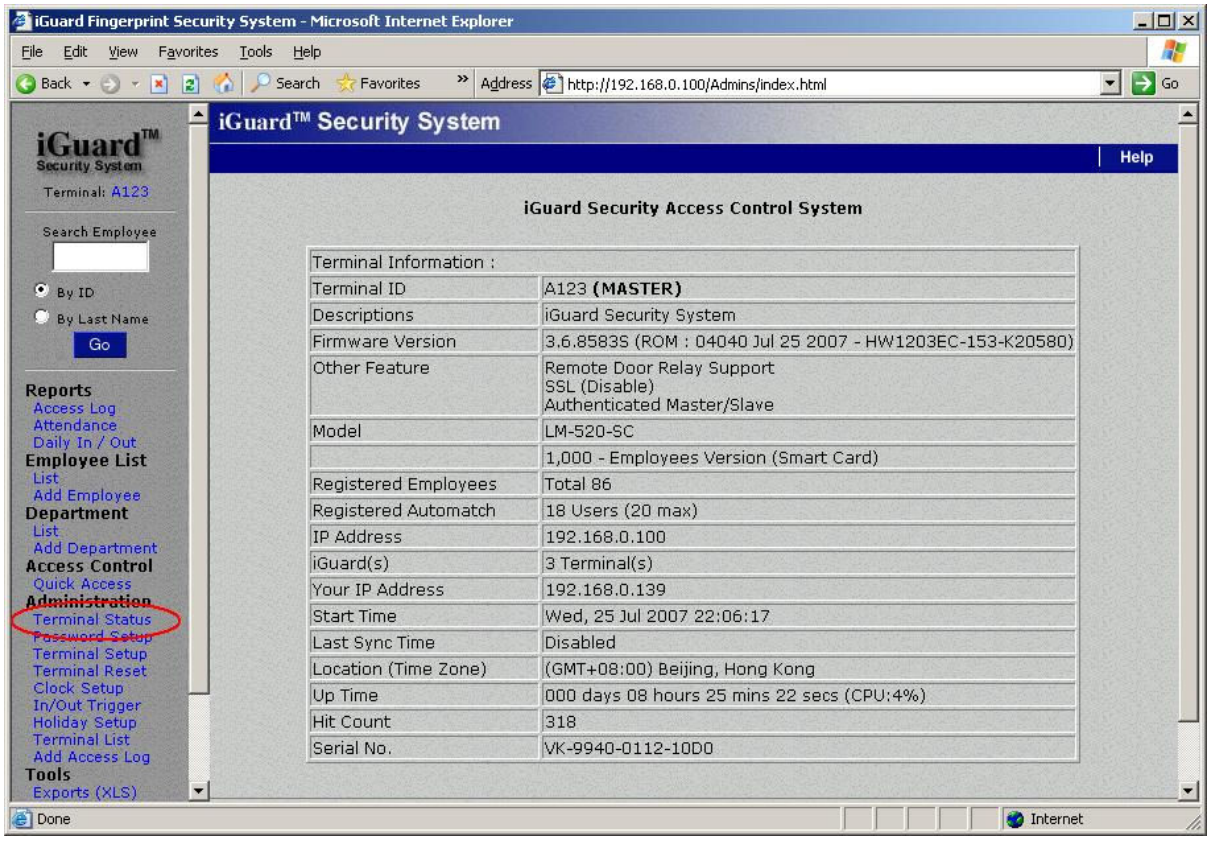
In the above example, Quick Access is available from 8:00AM until 6:30PM Monday through Friday, and never on Sunday, Saturday, and other specified company holidays.

Administration

This section will cover the settings and options for system configuration and maintenance.

Terminal Status

This is the iGuard homepage and the first page that will appear when accessing the unit with the Web Browser. The following is a typical *Terminal Status* page:



Terminal ID – shows the ID of the unit.

Terminal Descriptions – shows the description of the unit.

Firmware Version – shows the Firmware Version of the unit. The information is necessary should technical support is required in the future.

Other Feature – contains three entries. The first one, *Remote Door Relay Support*, indicates that this unit is equipped with the hardware interface for connecting to the optional *Remote Door Relay* unit (more detail can be found in the Appendix). The 2nd one, SSL, refers to the optional *Security Socket Layer* feature, which is a standard network security protocol for network communications between iGuards.

Note: The SSL is not a standard iGuard feature. It is available at extra cost. Please contact the manufacturer or the local dealer for more information in obtaining this feature.

The 3rd one, *Authenticated Master / Slave*, means that the System Administrator Password is required for Slave units to communicate with a Master unit. More on this can be found in the last chapter "*Keypad Operation → Function Menu → Func 0: Advanced Feature*".

Model – shows the model number of the unit.

Registered Employees & *AutoMatch* – show the number of the registered users and the number of AutoMatch-enabled users.

IP Address – shows the IP address of the iGuard unit.

iGuard(s) – indicates the total number of units that are connected together to form a Master / Slave network inclusively. If there is only one iGuard in the network, this number will be 1.

Your IP Address – refers to the IP address of the PC being used to browse the unit.

Start Time – records the start-time when the unit was first start up.

Last Sync Time – is used to indicate the last time the unit synchronized its internal clock with the SNTP Time Server (via the Internet). A SNTP Time Server can be specified in the *Terminal Setup* page (which will be discussed later) to allow the iGuard to synchronize the clock with.

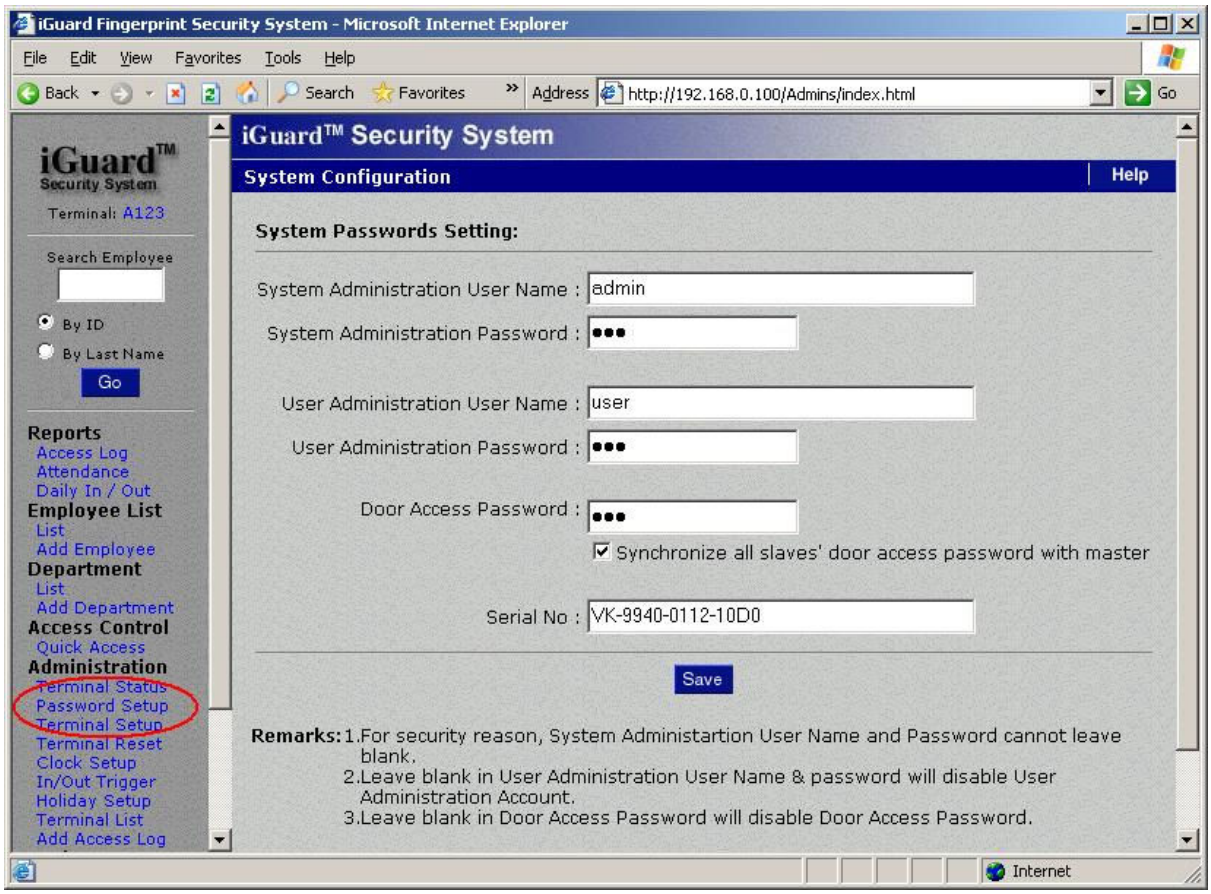
Location (Time Zone) – indicates the time zone the unit is in. It is for the time-zone adjustment when synchronizing the internal clock with the SNTP Timer Server.

Up Time – records the elapsed time when the unit was first powered on.

Serial No. – This is the Serial Number of the unit. The information is necessary should technical support is required in the future.

Password Setup

Use this page to set up the *System Administrator Password*, *User Administrator Password*, and the *Door Access Password*.



The first entry is the System Administrator's User Name & Password, which are required when accessing and modifying user information and system configuration. The valid characters for the password are 0-9, A & B, i.e., the characters one can enter using the iGuard keypad.

A Note on Master/Slave Configuration: The System Administrator Password of the Slave unit must be the same as the Master unit. Otherwise, the Master unit will reject the slave unit. In this case, an error message will be shown on the LCD display of the slave unit.

The second entry is the User Administrator's User Name & Password. This is for accessing and modifying the user information (e.g. to add and delete users, and to assign & modify departments). However, it cannot be used to access and modify any system-related configuration (e.g. to change the IP address of the unit).

The last entry is the Door Access Password, which is used for the Quick Access purpose (please refer to the *Quick Access* section earlier in this chapter in how to set up the Quick Access period).

The following steps illustrate how to use the *Quick Access Password* to gain access:-

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key. The unit will prompt you for the password.	`Enter Password:` `_`

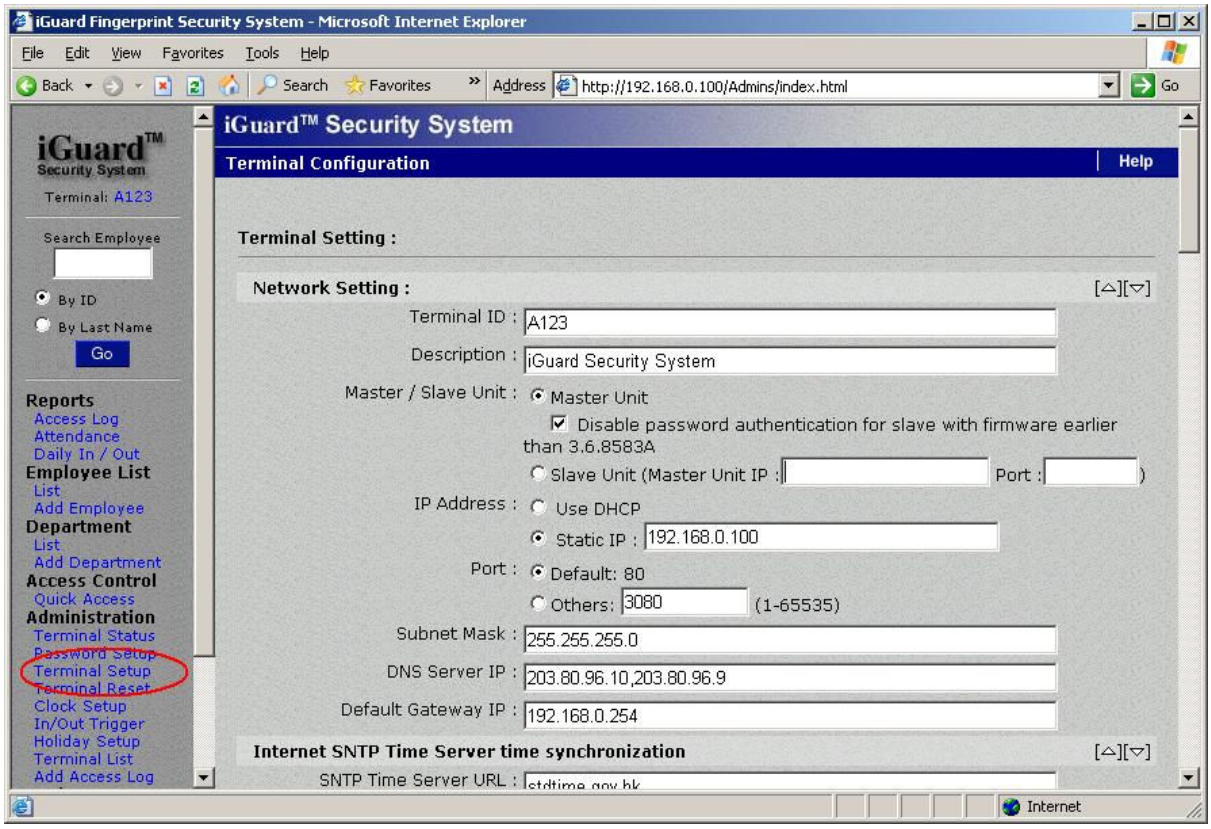
Description	***LCD Display***
2. Enter the *Quick Access Password.*	`Enter Password:` `******_`

3. Press **Func** key to confirm. If it is within the Quick Access Period, and this particular iGuard has been enabled for the Quick Access, the user will be authorized. The unit will return to Standby Mode.	`Authorized!`
	⋮
	`Thu Aug 30 15:02`
	`ID #:_ IN`

Unlike the other two administrator passwords, the Door Access Password can be configured as system-wise or unit-wise, by checking or clearing the checkbox of the "*Synchronize door access password with master*" option on the webpage. If it is configured as unit-wise, each slave can independently have its own Door Access Password.

Terminal Setup

Use this page to setup and configure the system. The following is a typical example of the *Terminal Setup* page:-



There are eleven sections in this page. These *are Network Setting, Internet SNTP Time Server, Other Options, Web Server Options, iServer, Fingerprint Matcher Setting, Door Relay and Beep Setting, Code Setting, Web Cam Setting, Weigand Setup* and *Remote Door Relay Setup*.

Network Setting

Terminal ID – Assign an ID to the unit. In a Master / Slave configuration, this Terminal ID is used to identify each slave unit in the network. Identical ID can be assigned to different iGuards. However, it is suggested to assign unique ID to each iGuard in a Master / Slave configuration, to avoid confusion when assigning departments' access right, in which the Terminal ID is used to identify which iGuard in the network is accessible by the department's members.

Description – Assign a descriptive name to the unit, for displaying in the "*Terminal List*" page.

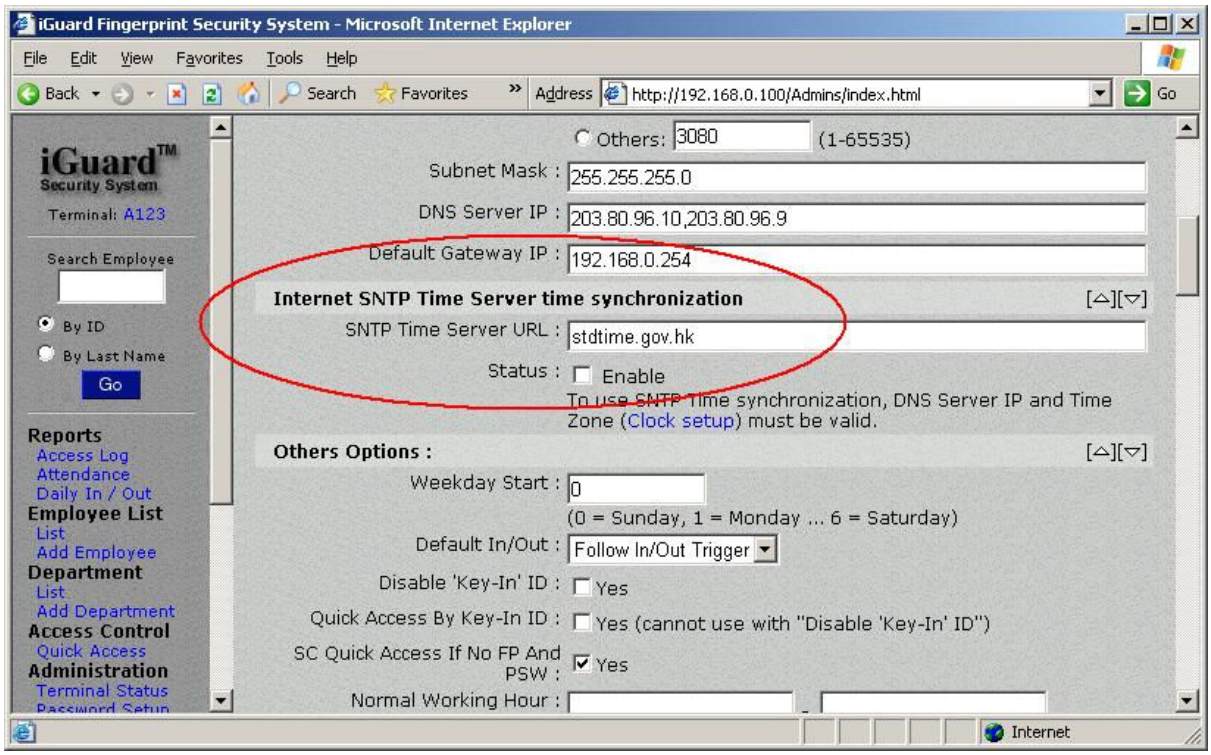
Master / Slave Unit – Each iGuard can be configured as a Master unit or a Slave unit by checking the corresponding checkbox here. For Master Unit, if there are slave units in the network that still run on firmware version older than 3.6.8583, the checkbox "*Disable password authentication for slave with firmware earlier than 3.6.8583*" must be unchecked. This is for backward compatibility purpose. Otherwise, the master unit will reject all these slave units running on the old firmware since these old slave units never notify the Master unit their System Administrator Passwords.

For Slave unit, the IP address and the Port number of the Master unit must be specified here.

IP Address, Port, Subnet Mask, DNS Server & *Default Gateway* – Specify the network settings of the unit. One can specify two IP addresses for the DNS server, separated by comma, as shown in the figure above.

Internet SNTP Time Server

SNTP stands for *Simple Network Time Protocol*. This allows the iGuard, if connected to the Internet, to synchronize it internal clock with one of the many atomic clocks on the internet, to ensure that the internal clock is always the most accurate.



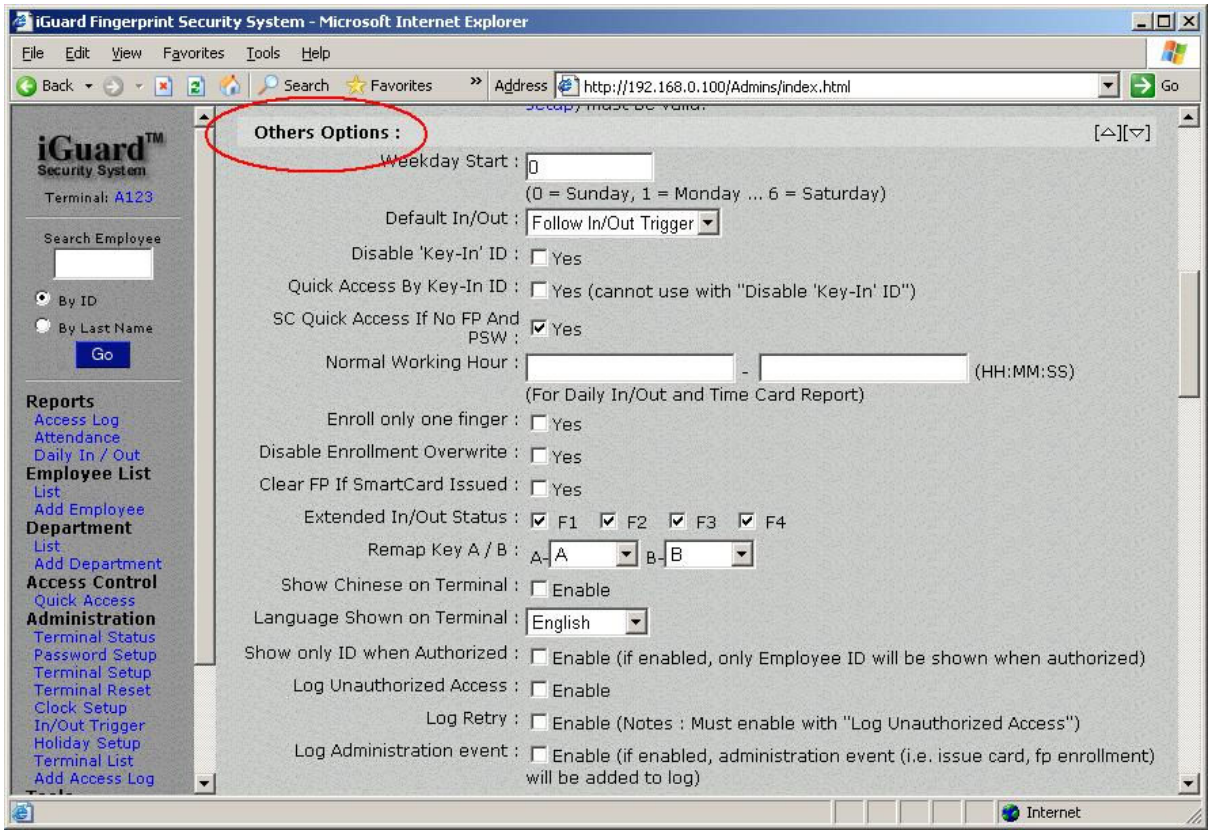
SNTP Time Server URL – Enter the URL of the SNTP Time Server. The default is *stdtime.gov.hk*.

Status – Check this checkbox to enable this feature.

In addition, one must also specify the *Time Zone* of the unit in the "Clock Setup" page located at "*Administration → System Clock Setup"*, which will be discussed later in this section. The DNS Server must also be properly setup to resolve the URL of the SNTP Time Server.

Other Options

This section contains several drop-down boxes and check boxes to configure how the Terminals will respond to user interaction.



Weekday Start – Use this to change the 1st day of the week from the default Sunday to others (useful for some Muslim countries and Hispanic).

Default In/Out – This is to define the default user access status, i.e., how the iGuard will log each clock event. iGuard assigns the access status to each access log entry, such as IN & OUT. The default access status is shown on the iGuard LCD display in Standby Mode. The available options are *Always IN*, *Always OUT*, *Follow In/Out Trigger*, *Don't Show, F1, F2, F3* & *F4*.

Except for the 3rd option, *Follow IN/OUT Trigger*, all the access log entries afterwards will be logged as the corresponding access status.

The *Follow IN/OUT Trigger* option allows the system to automatically update the default IN/OUT status depending on the settings configured in the *"In/Out Trigger"* page, which will be discussed later in this section. In this option, one can still change the default access status in an ad hoc basis by pressing the **Backspace** key on the keypad a few times to toggle the IN/OUT status, until the desired access status is shown on the LCD display.

Disable 'Key-In' ID – This is to disable the ability to use the keypad to enter user ID. This achieves a higher security level. If this option is set, the user must use his Smartcard or use the AutoMatch approach for verification, because he can no longer use the keypad to enter his ID for verification.

Quick Access By Key-In ID – If this option is enabled and it is within the *Quick Access* period, one can authenticate by entering the user ID without any means of verification. The user ID must be a valid ID found in the user database. This feature is mainly for convenience when the unit is used in an application where no security is required. Please

refer to *Quick Access* in the previous section for more information in configuring this *Quick Access* period.

SC Quick Access If No FP And PSW – If enabled, user can authenticate by presenting the Smartcard if no fingerprint template or personal password have been assigned to the person. However, if the user has enrolled his fingerprint or has been assigned a personal password, he still needs to submit the fingerprint image or enter the personal password for verification.

Normal Working Hour – Use this to specify the normal working hour, to allow the attendance report to show in red color the records that did not occur within this period.

Enroll only one finger – Reserved for backward compatibility. Do not enable this option.

Disable Enrollment Overwrite – By default, during the fingerprint enrollment procedure, the newly submitted fingerprint information will overwrite any existing one after confirmed by the user. This is to disable the overwrite capability. Once the fingerprint is enrolled for a user, the fingerprint information cannot be changed in any way later on. The main purpose for this feature is to avoid accidentally overwriting one's fingerprint information if a wrong user ID is entered during fingerprint enrollment.

If enabled, the administrator must delete a user and then re-create the user in order to re-enroll the user's fingerprint.

Clear FP If SmartCard Issued – This is mainly for privacy purpose. If enabled, the user's fingerprint information stored in the internal memory of the unit will automatically be cleared after issuing a Smartcard to the user. When issuing a Smartcard, all the user information, including the fingerprint information, will be written and saved in the Smartcard. By clearing the fingerprint information stored in the unit automatically, the user's Smartcard would be the only media that contains the fingerprint information, thus the privacy of the user can be protected.

During verification, iGuard will read all the contents of the Smartcard first, and then it will compare the fingerprint information saved in the Smartcard against the submitted fingerprint image.

Extended In/Out Status – Four additional access statuses, F1 to F4, are available as well as the normal IN and OUT status. Enable any one or all of these four additional access statuses by checking the corresponding checkboxes.

As an example, assign F1 as *Lunch Out*, and F2 *as Lunch In*, so the employees can use F1 when they are out for lunch, and use F2 when they are back from lunch.

Remap Key A/B – Normally the **Backspace** key on the keypad is used to scroll through all the possible access statuses, i.e., IN, OUT, F1… etc., and to select the desired one. This option is for assigning the two shortcut keys, A & B, to these access statuses, so the user can just press these keys, instead of pressing the **backspace** key numerous times, to select the desired access status.

However, please note that once assigned to the access status, these two keys can no longer be used to enter any normal user ID.

Show Chinese on Terminal –Reserved. Do not enable this option (not available in US models).

Language Shown on Terminal – Reserved. Do not change this option (not available in US models).

Show only ID when Authorized – If enabled, the user ID, instead of user name, will be shown on the 1st line of the LCD display when authorized, to avoid disclosing the user name to others standing in the line.

Log Unauthorized Access – By default, the access log only records the successful authentication. If this option is enabled, the system will also record all the unsuccessful attempts and store these records in the access log.

These unsuccessful attempts include events like using the wrong finger, attempting to access a unit which he does not have permission to access, an inactive user attempting to access the unit, and others. But this will not log activity for non-users (such as the *"Invalid ID"* attempt).

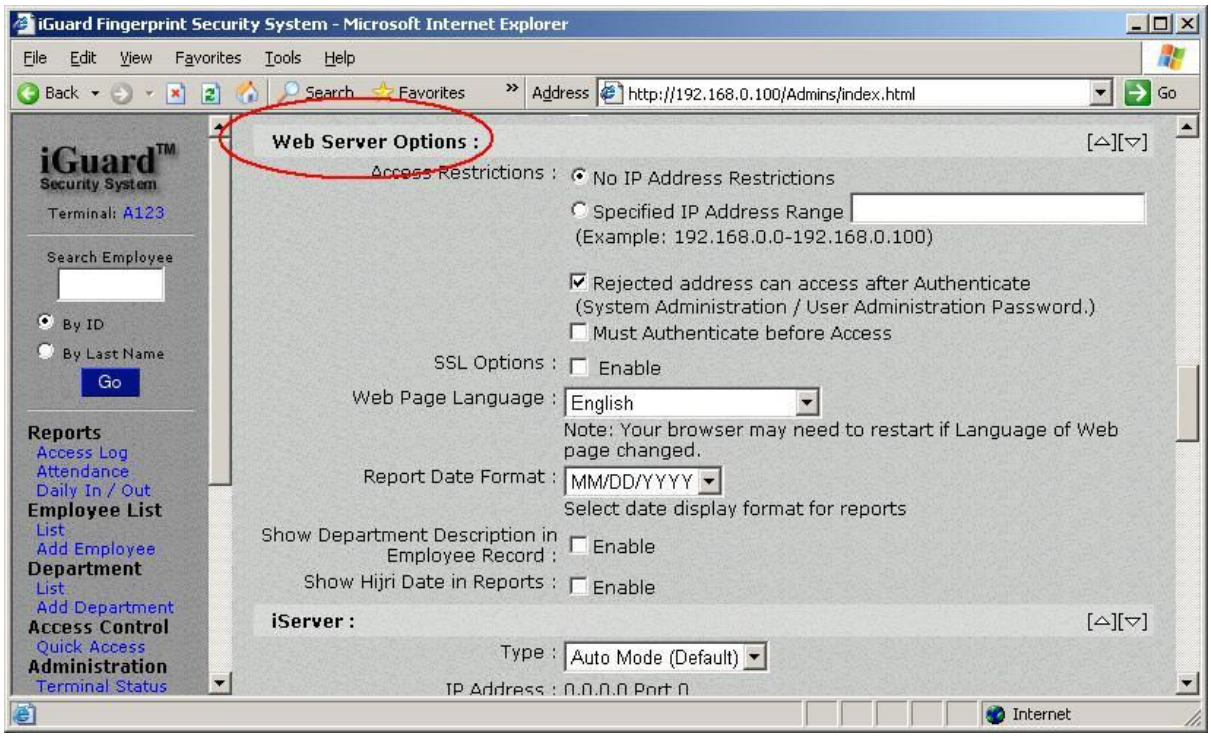
Log Retry – During the fingerprint verification, if the submitted fingerprint does not match the fingerprint template, the user will be asked to resubmit his fingerprint. Again, by default, this incident will not be recorded in the access log. If this option is enabled, the access log will include these "retry" events.

This is useful for identifying users who are consistently getting fingerprint false rejections and have to attempt access multiple times. These people may have fingerprints which are difficult to read, or may not have been enrolled properly.

Log Administration Events – If enabled, the access log will includes all the administration events, such as adding, modifying and deleting users.

Web Server Options

This is to set various web server-related options.



Access Restrictions – This setting allows you to specify a specific IP address, or a range of IP addresses that is authorized to access the iGuard unit. Select the default "*No IP Address Restriction*" to allow any IP address to access the system. To restrict a specified range of authorized IP address, select the 2nd one, "*Specified IP Address Range*", and enter the range to the box next to it.

The 2nd option, "*Rejected address can access after Authenticate*", is for allowing a rejected IP address to access the iGuard's via web browser by providing the System Administrator Password.

The 3rd option, "*Must Authenticate before Access*", is to force the iGuard to ask for System or User Administrator Password for all web access, including the Access Log and other reports, even if the IP address of the PC is within the IP range specified above (by default, password is not necessary to access the Access Log and other reports).

SSL Options – This option is not available in standard iGuard. Please contact the dealer or the manufacturer if this option is needed.

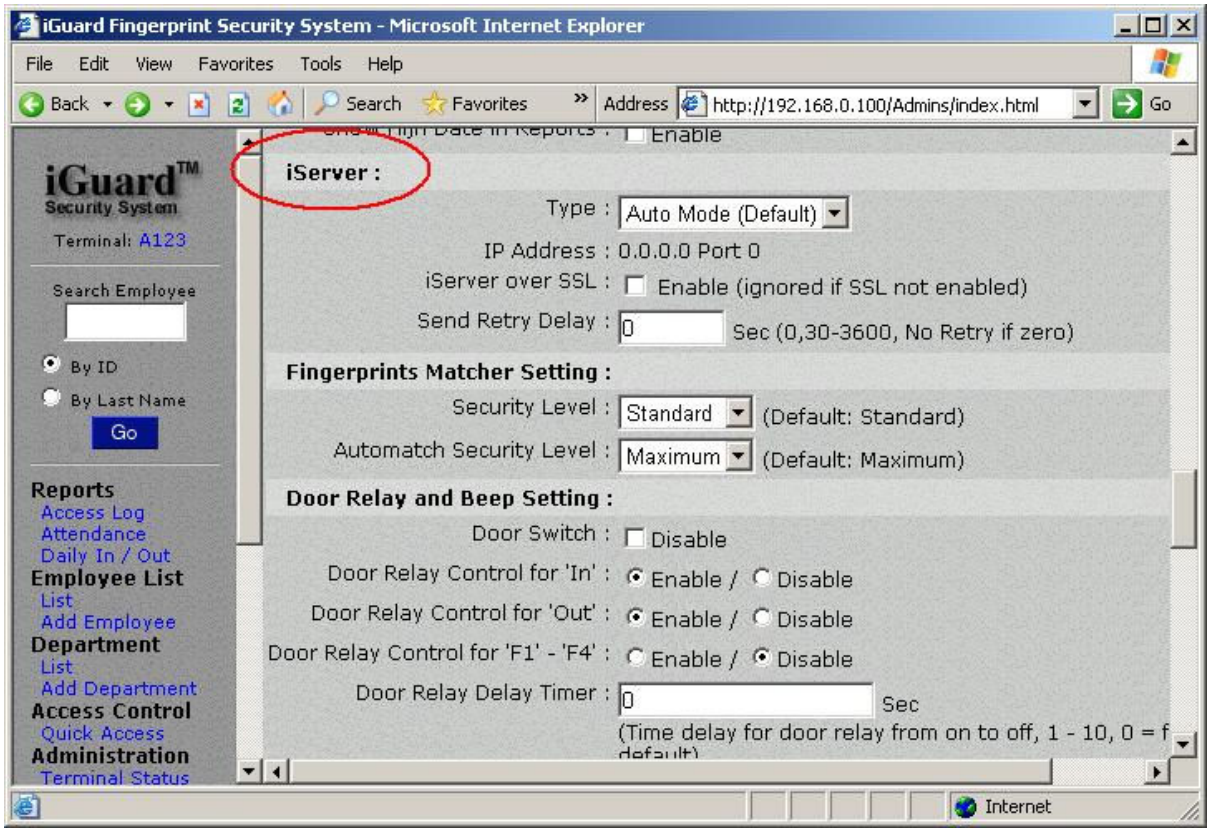
Web Page Language – This is to select the webpage language from the list. Please contact the dealer or the manufacturer if the desired language is not on the list.

Report Date Format – Select the desired date format from the list. Available date formats are MM/DD/YYYY, MM-DD-YYYY, DD/MM/YYYY and more.

Show Department Description in Employee Record – This is to include the Department Description field in the Department List in the *Employee Record* page. The maximum length of the Department ID is only 8 characters long, so in some cases it would be helpful to also include the description for clarity purpose.

iServer

This is to configure iGuard to work with the iServer program.



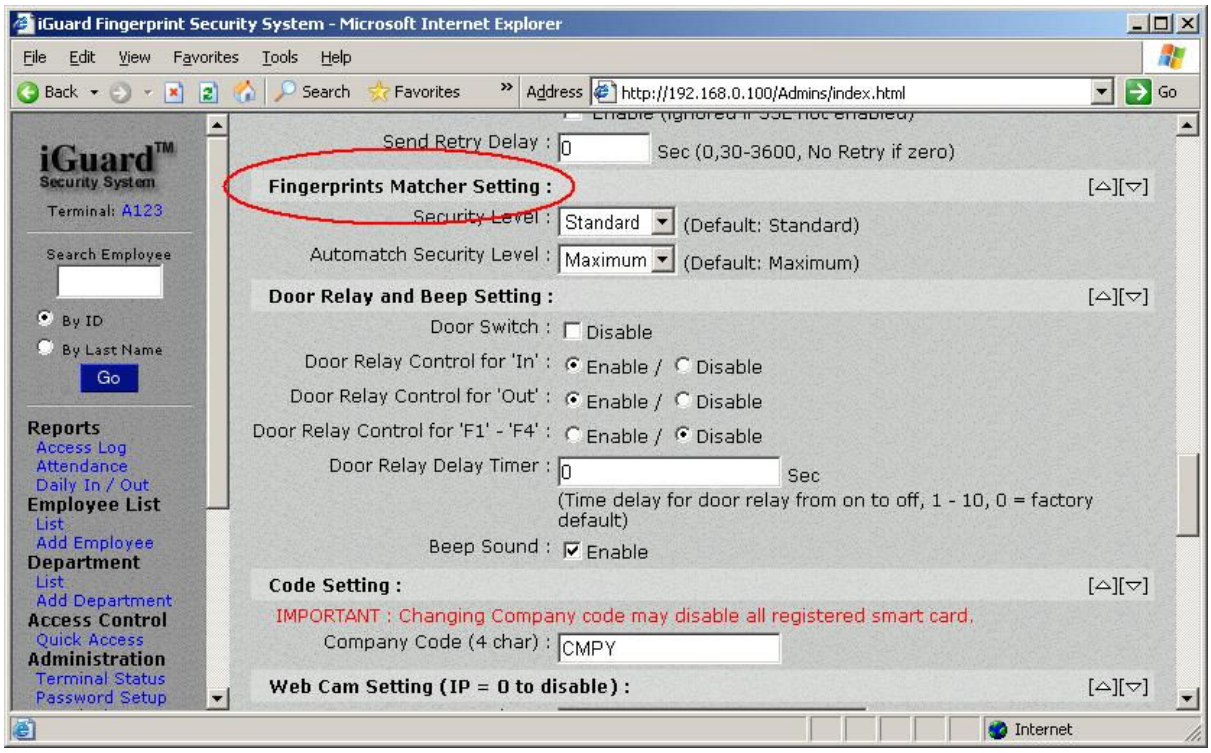
Once enabled, iGuard will send all the access log records to the PC running the iServer program, and all the records will be saved in the PC hard disk permanently. The transmission is in real-time manner.

The iServer program can be downloaded free of charge in the manufacturer's website. More detail about iServer will be covered in the Appendix.

Important: Always set the first option, *Type*, to "Auto Mode", and leave the other options unchanged, to work with the current version of iServer program.

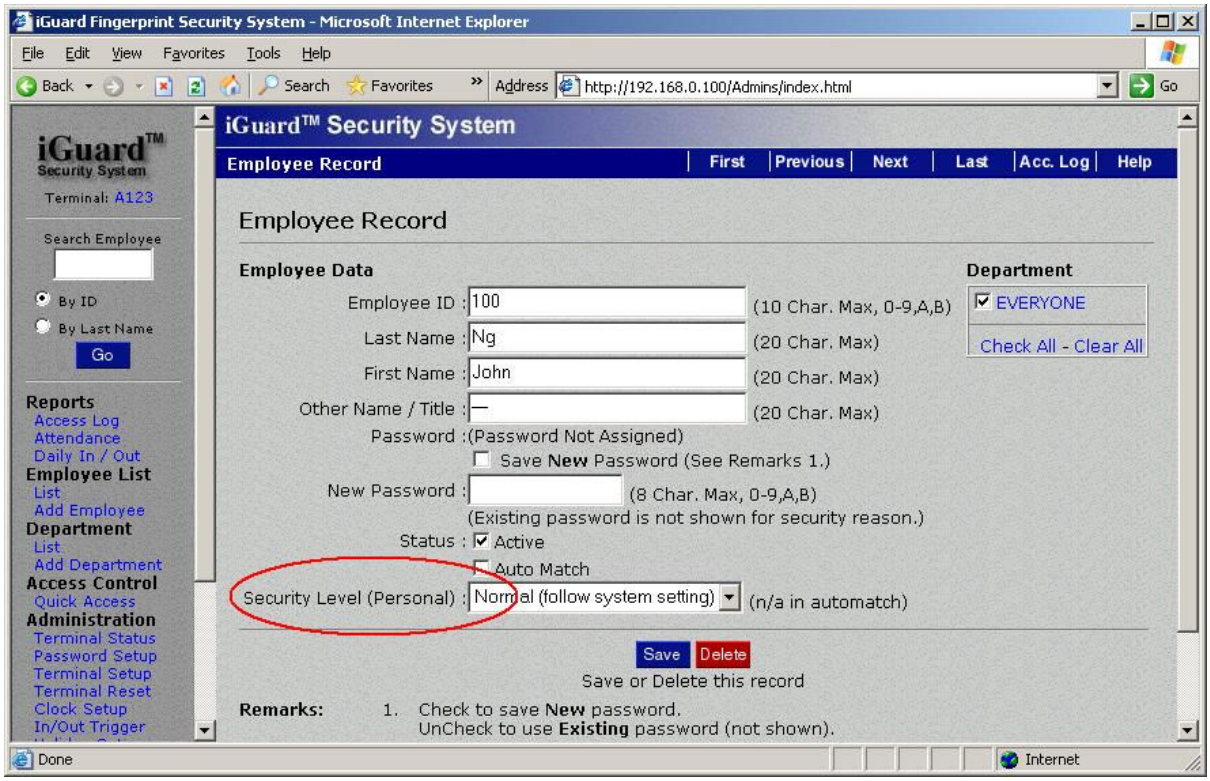
Fingerprint Matching Setting

This is for setting the security level for fingerprint matching for the system (applicable to iGuard with the optional fingerprint sensor only):



In most cases, use the default settings for optimum performance.

<u>*Security Level*</u> – This is the System Level setting that specifies the security level iGuard would use for a user if the Personal Security Level for the user is set to "*Normal (follow system setting)*", as shown in the following figure:

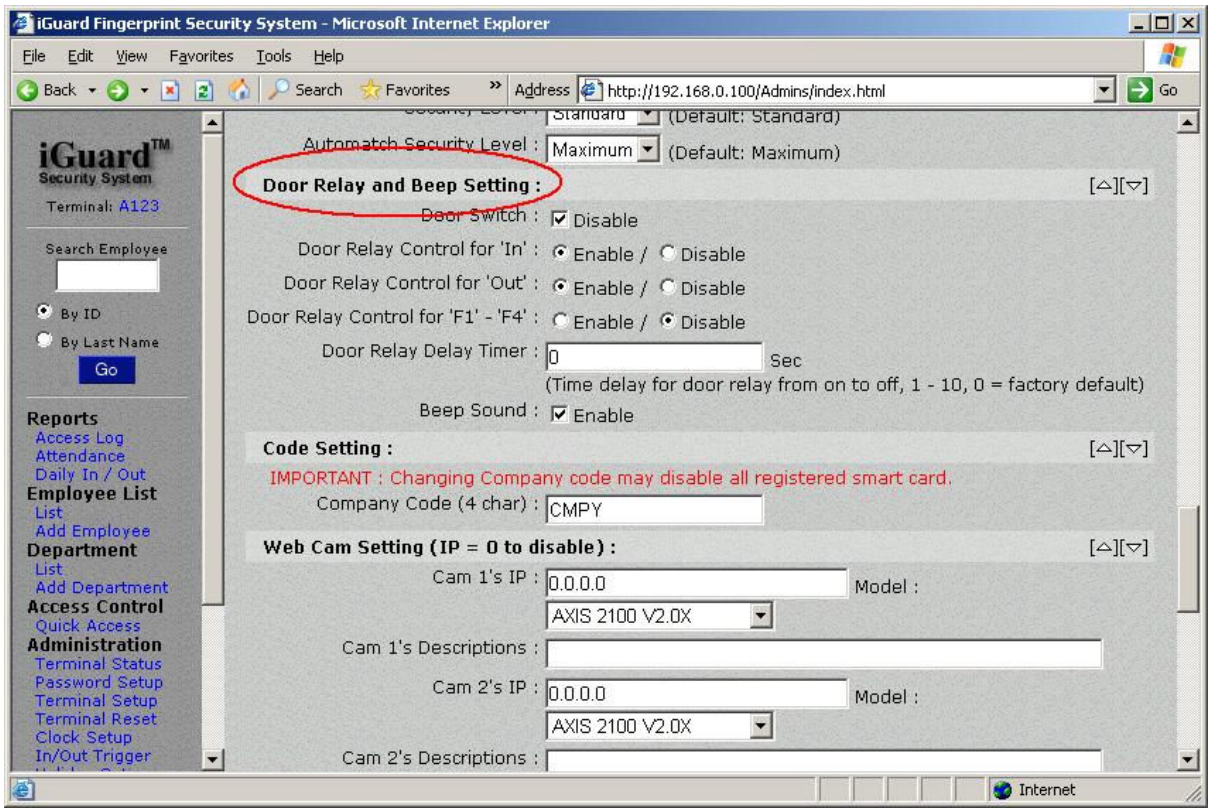


Other *Personal Security Level* settings would overrides the System Level setting above.

AutoMatch Security Level – This is to specify the fingerprint matching security level used during the AutoMatch (i.e., 1 - to - many) operation. Set this to *Maximum* to avoid false-acceptance error.

Door Relay and Beep Setting

This is to configure the various options for controlling the door relay. Use these options to configure which type of events should or should not open the door.



Door Switch – Reserved for backward compatibility. Always set it to "Disable".

Door Relay Control for 'IN' – If enabled, the built-in door relay will be switched on for all successful clock-in accesses. This is also applicable to the optional *Remote Door Relay* unit (which will be discussed in the Appendix).

Door Relay Control for 'OUT' – This is the same as the 'IN' counterpart discussed above, except it is for the 'OUT' access status.

Note: This option is useful if the device is installed outside of the main door of the premises, and the device is used for both access control and time keeping purposes. By disabling this option, the door will not open if someone clocks-out from the device when leaving the place.

Door Relay Control for 'F1' - 'F4' – This is the same as the 'IN' counterpart discussed above, except it is for the 'F1', 'F2', 'F3' & 'F4' access status.

Door Relay Delay Timer – This is to specify the duration (in second) of the door relay when it is switched on. The default is 3 seconds. Set this to a larger value if the iGuard is

not installed immediately next to the door, and the user may take a few seconds to reach the door after being authenticated.

Beep Sound – Use this to enable / disable the built-in beeper, which is useful if quiet operation is required.

Code Setting

This is for Smart Card operation only.

This Code is a 4-character string that will be written to all smartcards issued by the unit. The default is "CMPY". When reading the card, iGuard will first compare the smartcard's code against the device's code. If they do not match, iGuard will just simply ignore the card.

Warning: This value must be set prior to issuing any smartcard, and must not be changed afterwards. Otherwise, all previously issued smartcards will be ignored.

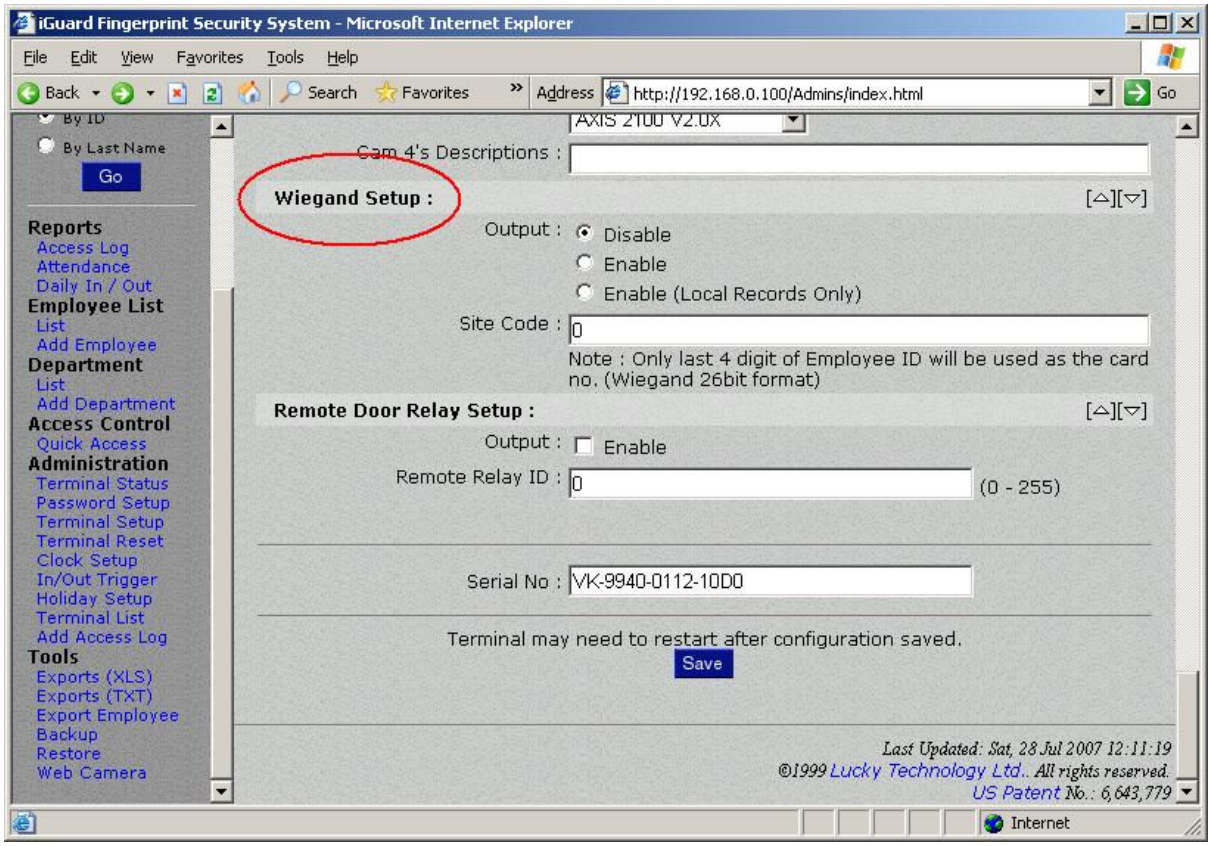
Web Cam Setting

This section allows you to configure up to four cameras to be viewed from within the iGuard interface. The cameras must be IP capable, and will be visible from the "*Web Camera"* page under the "*Tools"* section. iGuard will display the streaming video for 120 seconds at a time, and will not record. This feature is only for viewing.

Use the pull-down menu to select the web cam models. Please contact the manufacturer if the desired web cam is not in the list.

Wiegand Setup

iGuard can be used as a Wiegand Output Reader. There is a Wiegand output connector at the back of iGuard which outputs the user ID to another Wiegand device in the standard 26-bit format.



Output – Enable this setting if it is necessary to connect iGuard to any existing Wiegand-based system. To include only the local access log records (i.e., to exclude the access log records from other slave units), check the last option "*Enable (Local Records Only)*".

Site Code – This is the Wiegand site code. Use this setting to communication properly with existing Wiegand systems.

Remote Door Relay Setup

This is for setting up the optional *Remote Door Relay*, which is a small device for controlling the electric door strike.

Normally, the electric door strike is connected directly to the built-in door relay of the device. For higher security purpose, this Remote Door Relay can be used instead of the built-in one to control the door strike, to avoid the possible intruder break-in by opening the iGuard and directly shorting the door strike wires.

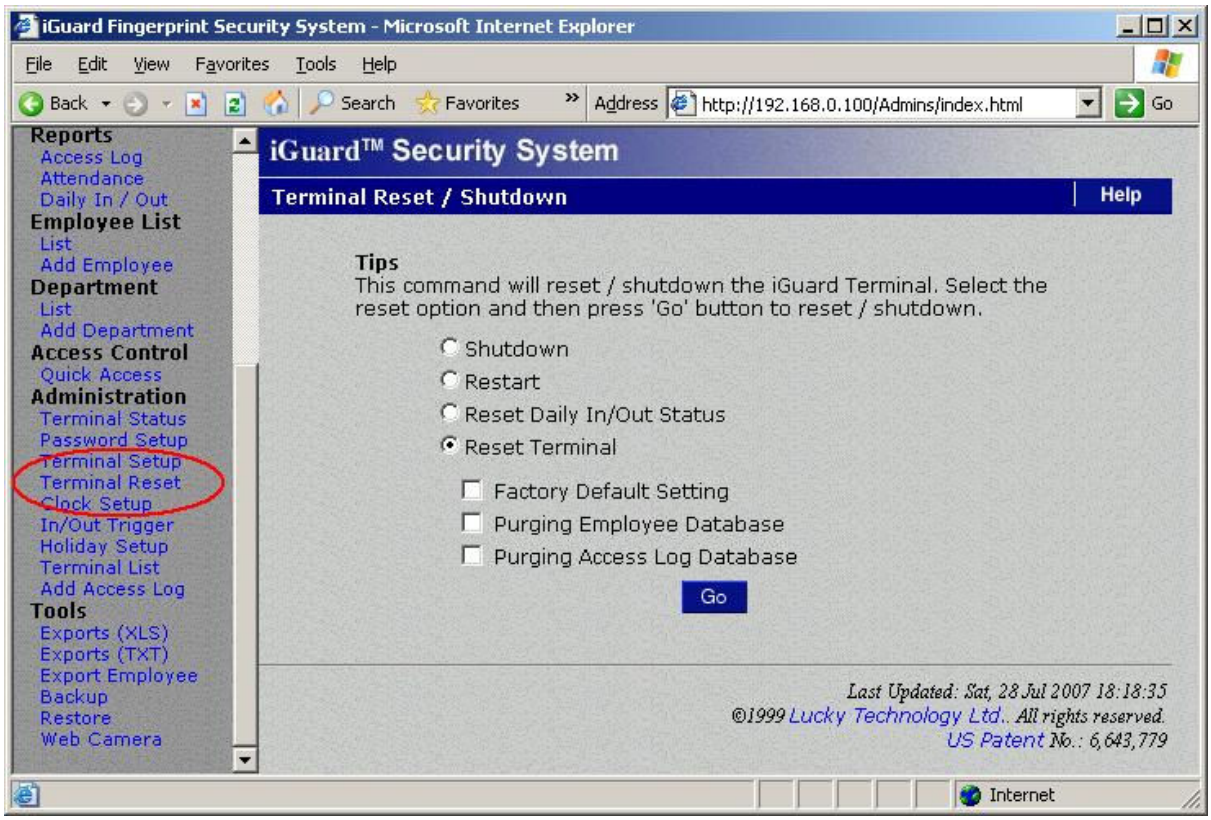
More details will be discussed in the Appendix.

Output – Enable this if the optional Remote Door Relay is available.

Remote Relay ID – This number must match the 8-bit jumper block setting located on Remote Door Relay device.

Terminal Reset / Shutdown

Use this page to remotely reset or shutdown the iGuard.



Press the Go button at the bottom to reset the device according to following selections:

Shutdown – This is to simply shut down the device. The device can be restarted again by pressing any key on the keypad.

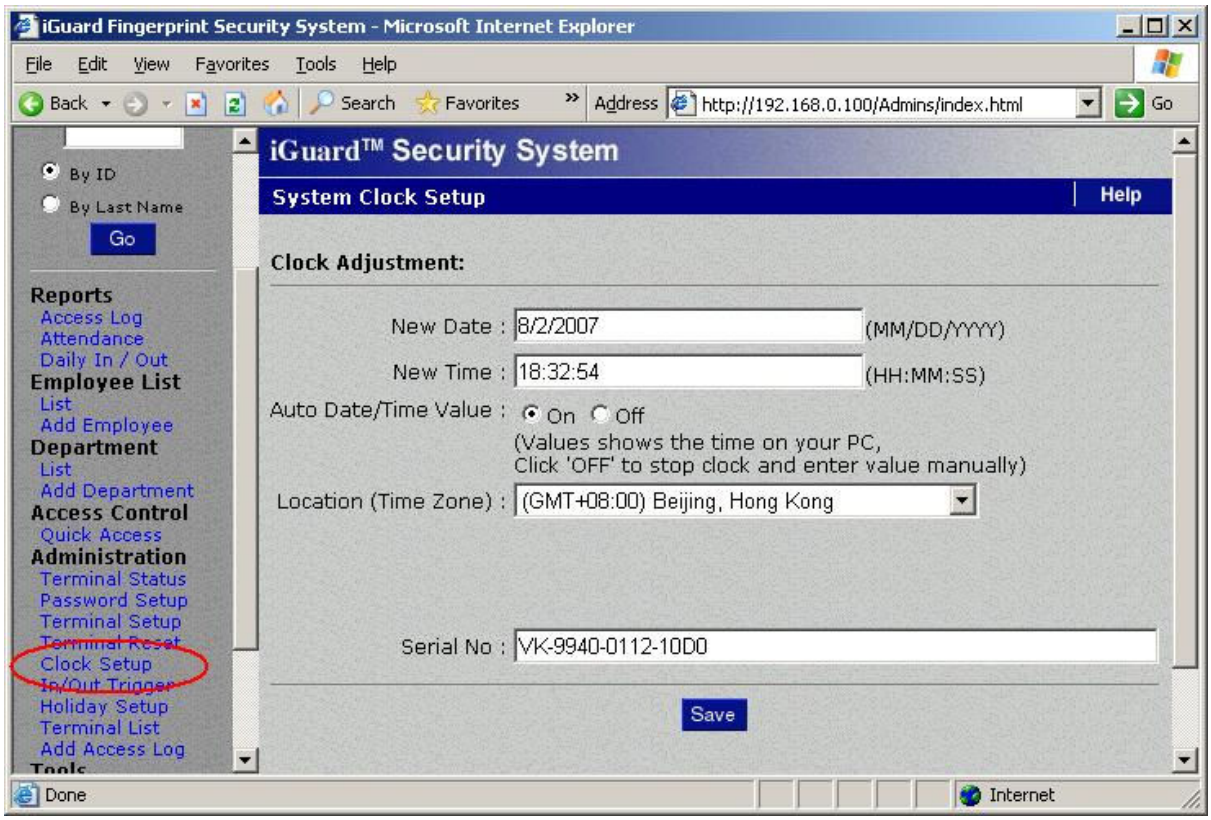
Restart – Select this one to restart the device.

Reset Daily In/Out Status – iGuard keeps a list of all users' most recent IN/OUT status and the corresponding date & time information. View this on the webpage in the "*Employee List*" page discussed earlier. Use this option is to clear the information.

Reset Terminal – This is for restoring all the device settings to factory default, and to reset the user & and access log database. This is analogous to the *Function 7: Shutdown / Reset* in the keypad function menu discussed earlier.

System Clock Setup

Use this page to update the system clock.



New Date / Time – Enter the new date and time here. This page uses the current time in the PC as the default date and time values, and the time is continuously being updated. Simply press the "Save" button to accept the default time. To manually input the date and the time, check the "*Off*" checkbox to stop the update, and then enter the new date and time manually.

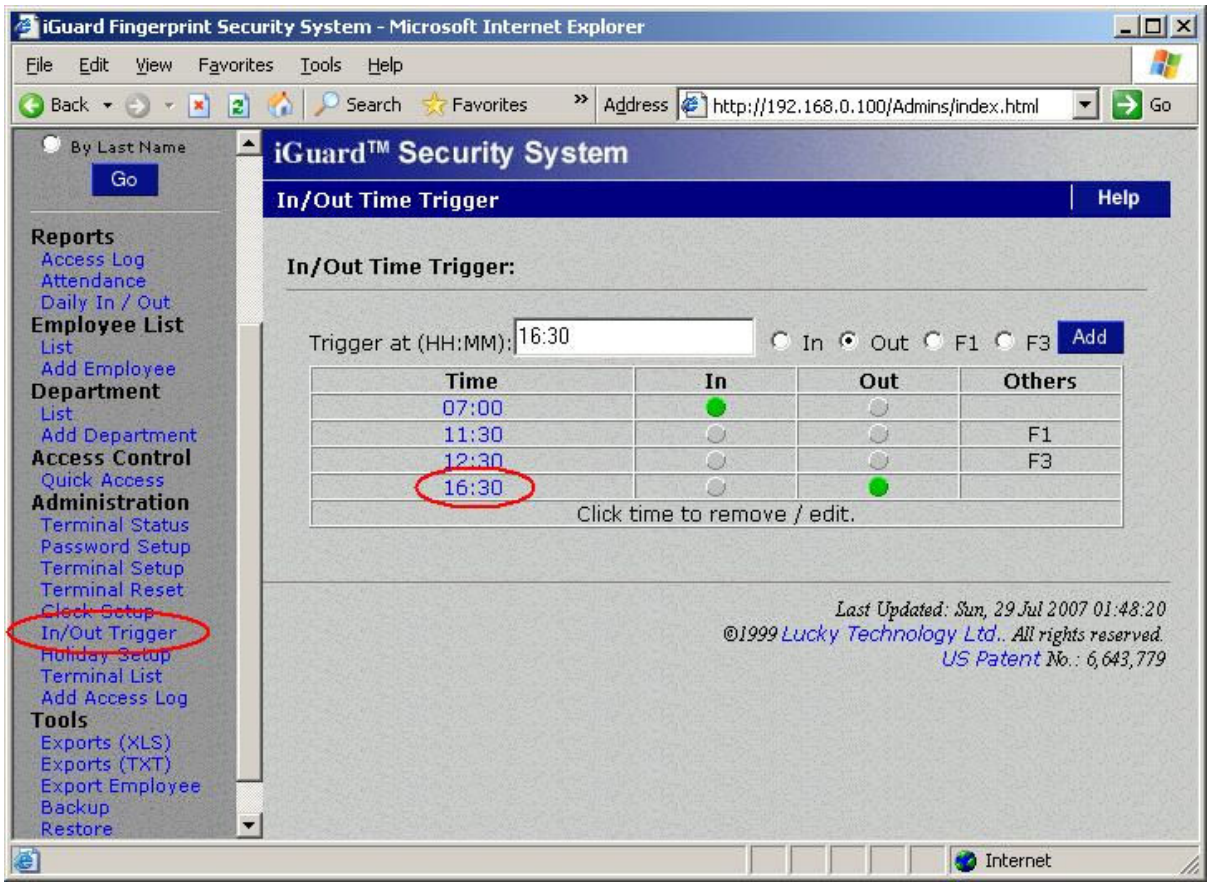
Auto Date/Time Value – This is to continuously update the two Date & Time fields above. To manually enter the date and time, turn off this option by checking the "*Off*" button.

Location (Time Zone) – This setting is applicable to the *SNTP Time Server*, and must be correctly set according to the local time zone. This setting is important if the *SNTP Time Server* has been specified in the "*Terminal Setup*" page. This setting is also required for clock synchronization between master and slave units.

In/Out Time Trigger

Use this page to set triggers for the IN / OUT setting. At the specified time, the default access status will automatically set to IN, and the unit clocks-in anyone who accesses the unit. The same applies for other access statuses like OUT, F1, F2 … etc.

The following is a typical example of the setup:-



In this example, when the time reaches 7:00 in the morning, the default access status will change from OUT to IN. Likewise, the device will change the default status to F1 at 11:30, to F3 at 12:30, and to OUT at 16:30, as shown in the following:-

Description	***LCD Display***
1. The default access status is OUT at 6:59	`Thu Aug 30 06:59` `ID #:_ OUT`

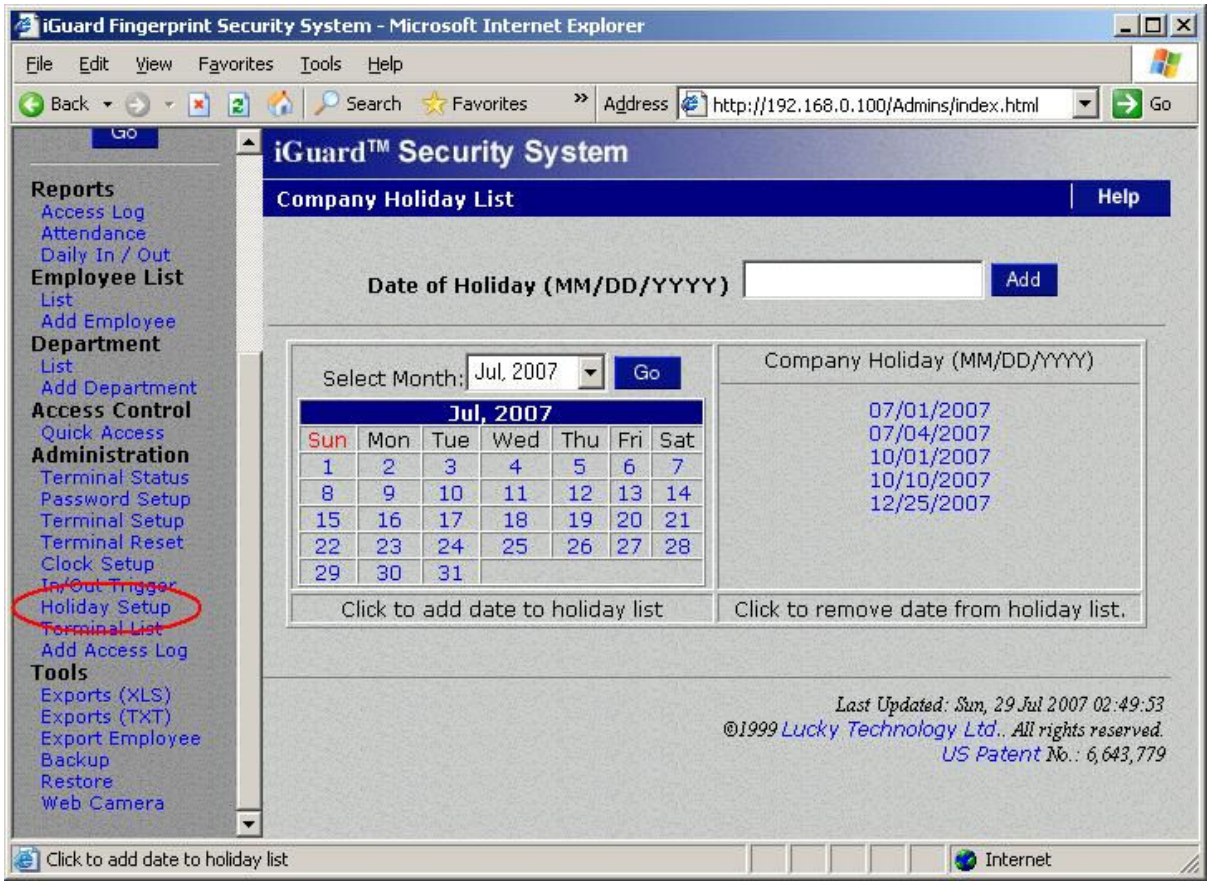
2. The default access status changes to IN at 7:00, to F1 at 11:30, to F3 at 12:30, and back to OUT at 16:30.	`Thu Aug 30 07:00`
	`ID #:_ IN`
	⋮
	`Thu Aug 30 11:30`
	`ID #:_ F1`
	⋮
	`Thu Aug 30 12:30`
	`ID #:_ F3`
	⋮
	`Thu Aug 30 16:30`
	`ID #:_ OUT`

The entry can be removed by simply clicking on the blue *Time* link, which is circled in red in the above figure for illustration purpose.

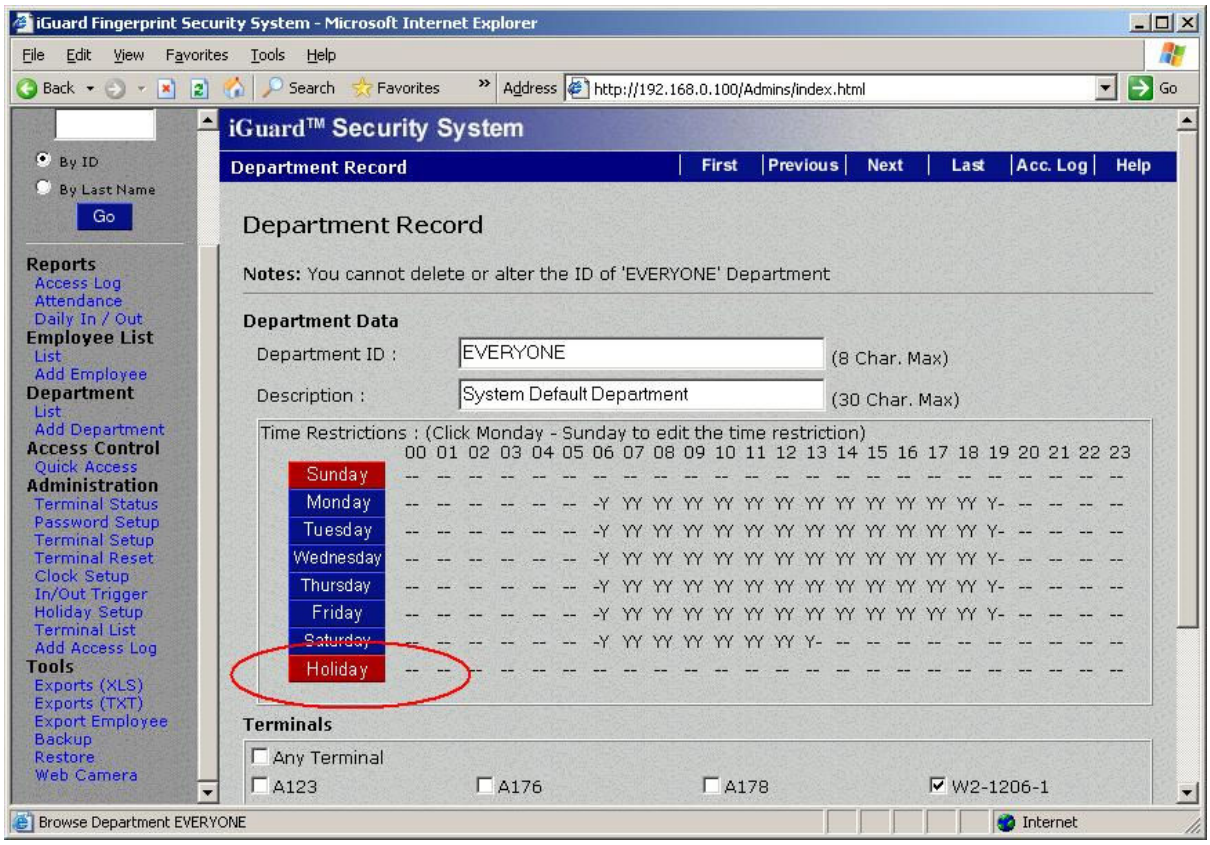
Note: The user can always override this default access status by pressing the *Backspace* key a few times until the desired access status is displayed on the LCD before entering the ID.

Holiday Setup

Use this page to establish the Company Holiday List. The Holiday list is used for the *time restriction* purpose (along with the day-of-week settings) for access right control. The following is a typical example of the setting:-



In the above example, the dates 07/01/2007, 07/04/2007, 10/01/2007, 10/10/2007 & 12/25/2007 are set as holidays. On these days, the authorized time period will follow the settings for the date "*Holiday*", as shown in the following: -

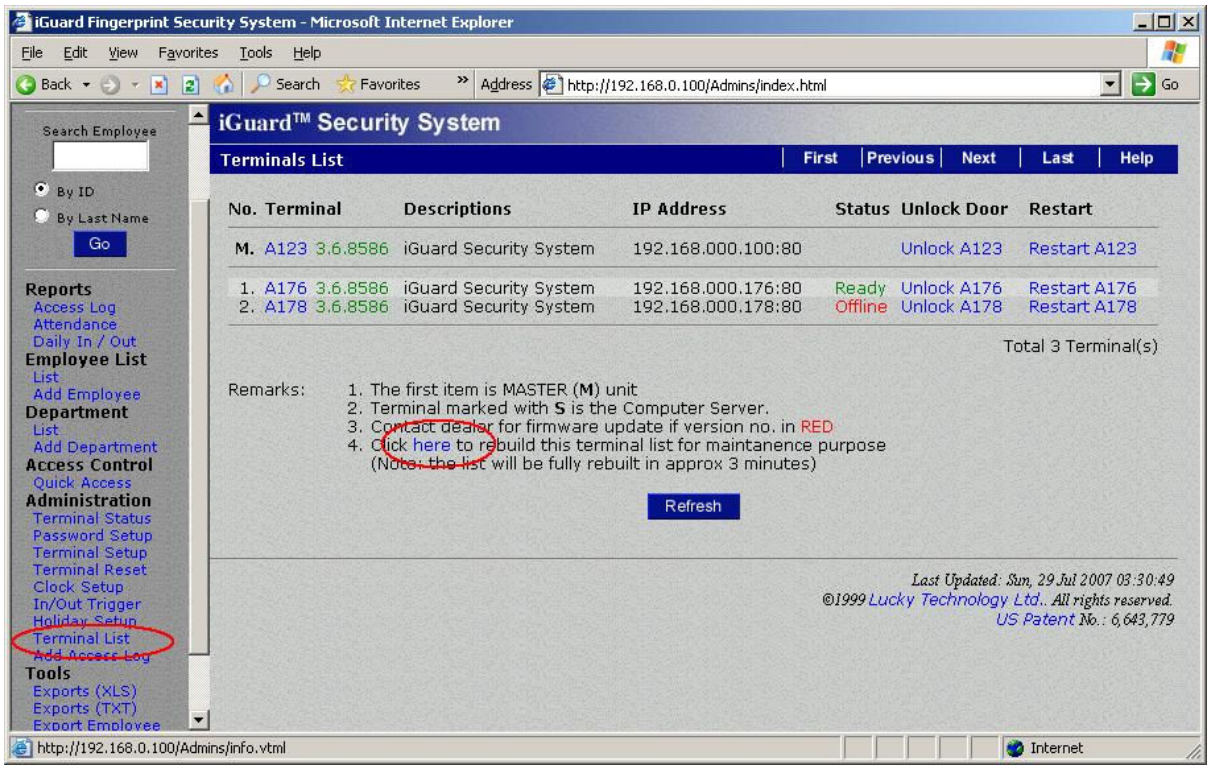


In the above example, no one would have the access right during the 5 holidays specified above.

To remove a holiday from the list, simply click the blue date in the ‘Company Holiday’ list.

Terminal List

This page shows the current slave units in the master / slave network: -



In the above example, the device “A123” is the master unit, and it has two slave units with terminal ID “A176” & “A178”.

The corresponding *Firmware Version*, *IP address* & the *Port number* are also shown.

The *Network Status* column indicates the network connection status. In the above example, the slave unit “A178” is offline.

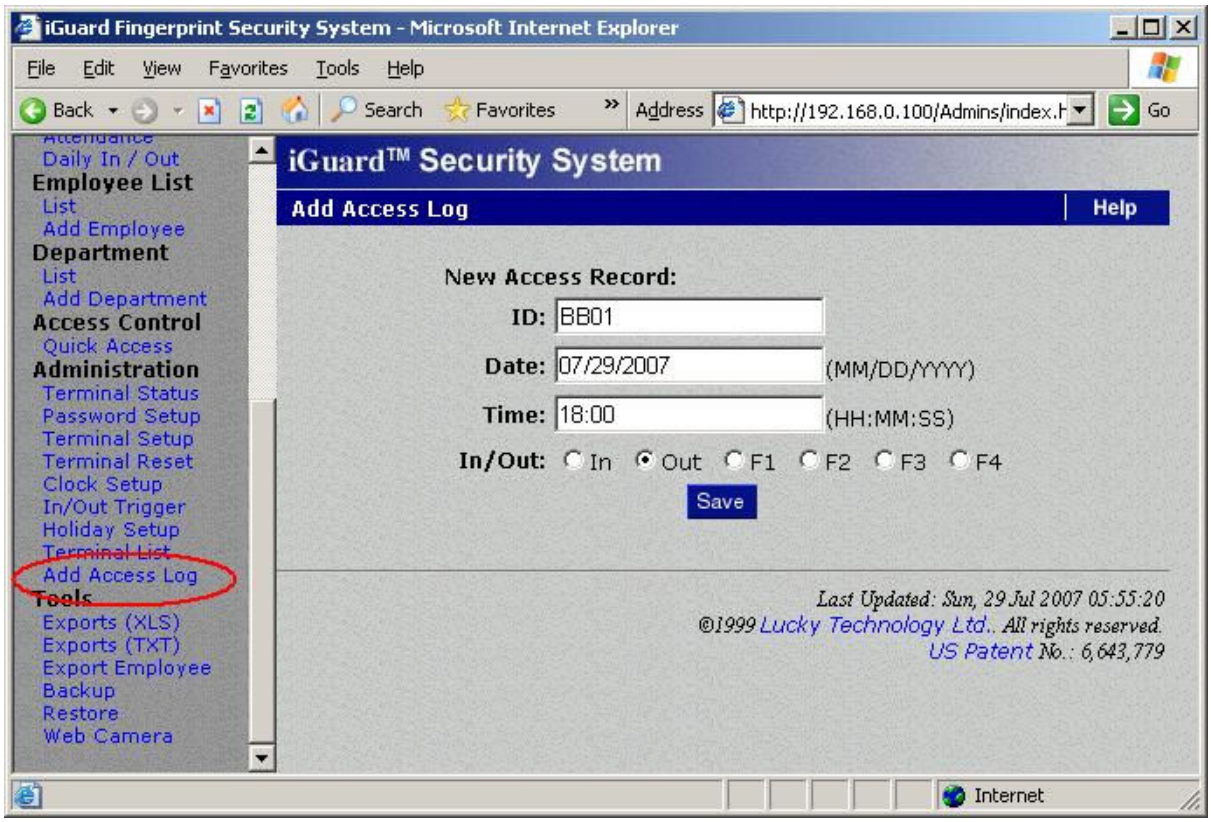
As a convenient feature, one can remotely unlock the doors of the slave unit or reset the slave unit by clicking the *Unlock* & *Restart* links respectively.

To clear the terminal list, click on the link at the remark #4 (circled in red above for easy reference). Each slave unit will regularly send an acknowledge signal to the master unit. Once this acknowledged signal is received, the master unit will add the slave unit to the list again.

One can test the network connection against all the slave units by pressing the “*Refresh*” button at the bottom of the page. The unit will then try to “ping” each slave unit one by one, and if the network connection with a slave unit is lost, this slave unit will be cleared from the list. This operation may take a long time if there are a lot of slaves in the list under slow network connections.

Add Access Log

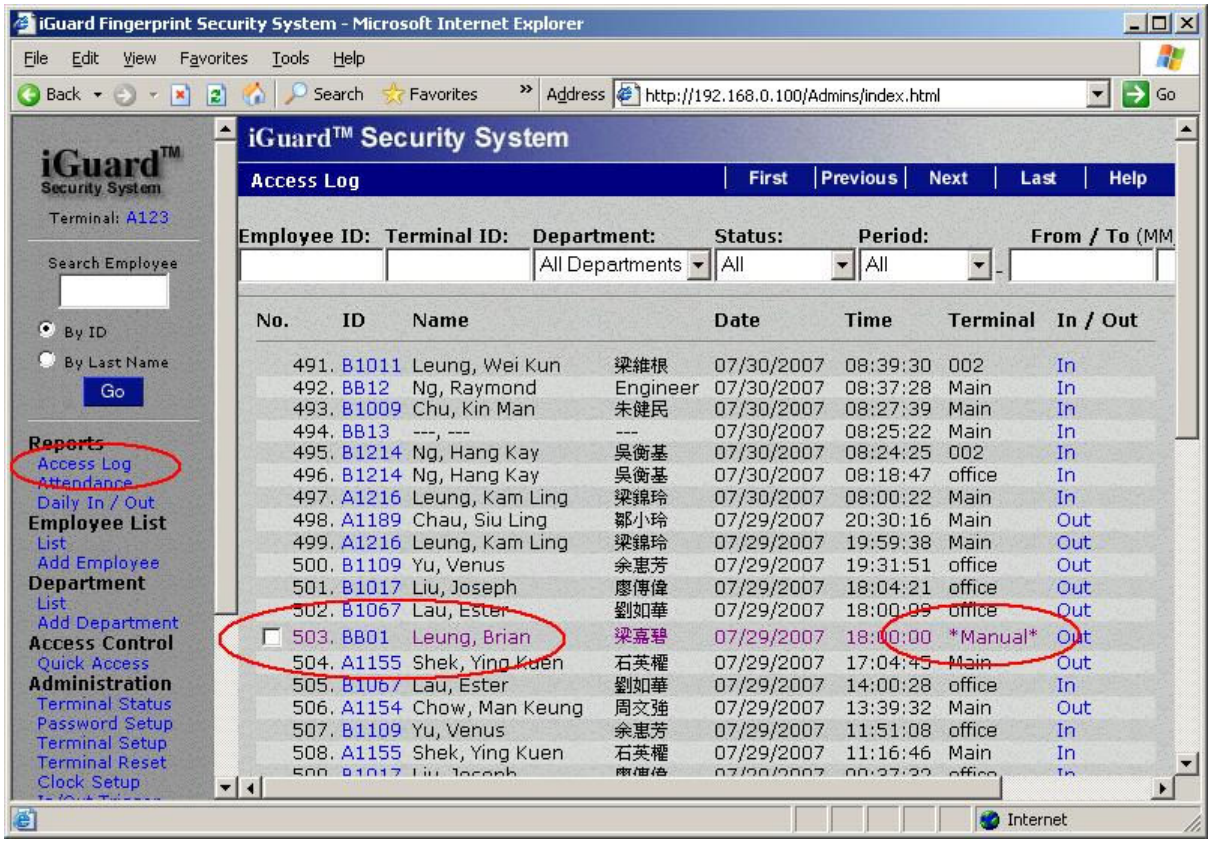
Use this page to manually add an access log entry: -



It is sometimes necessary to add a record manually for an employee. For example, the employee might have forgotten to clock-out before going home at the end of the day, and so it is necessary to make up for the mistake by manually adding this entry back, which is particularly useful for payroll purposes.

By default, only access records which have been manually added can be changed or deleted.

In the above example, an entry for user BB01 will be manually added to the access log, and the access log report will become: -



Access logs which have been added manually will have a check box next to them and will be shown in purple. They will also say **Manual** in the "*Terminal*" column of the record. These are the only records which can be deleted from the system. To delete these records, select them by checking on the check boxes and press the *Delete* button at the bottom of the page.

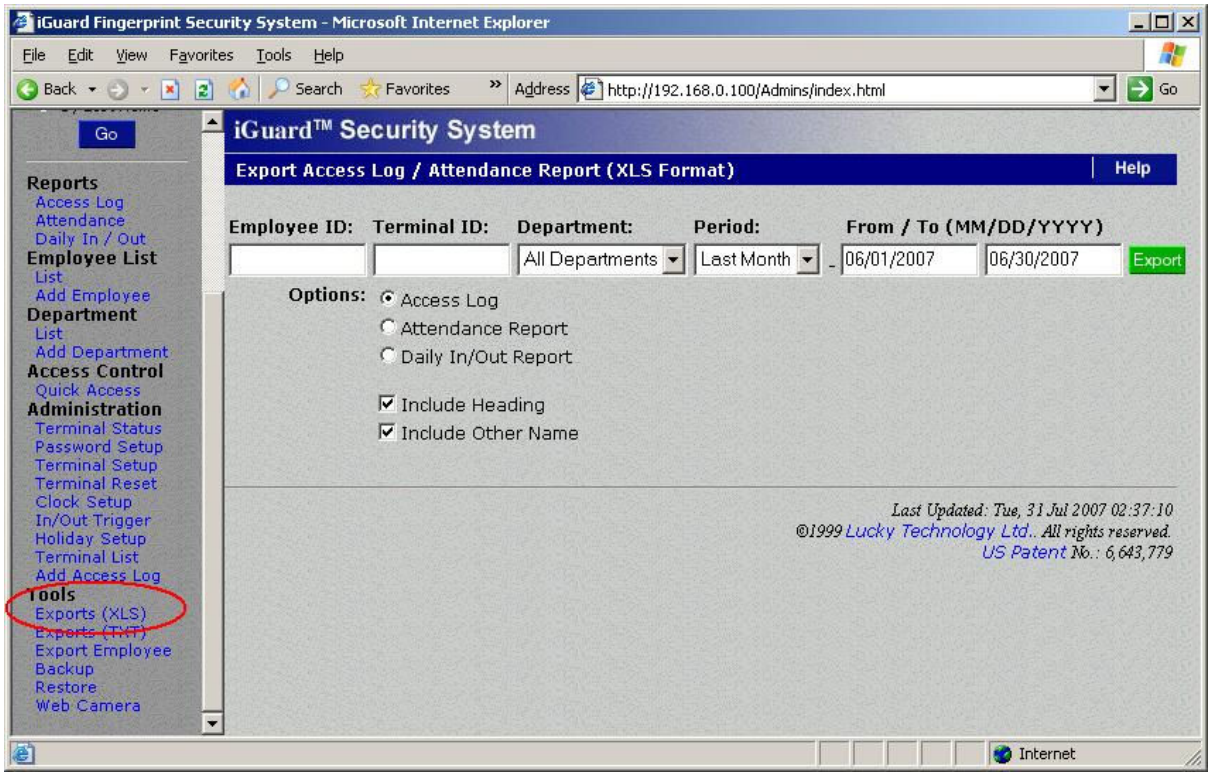
Note: Only manually-added records can be deleted. All other records are irrevocable.

Tools

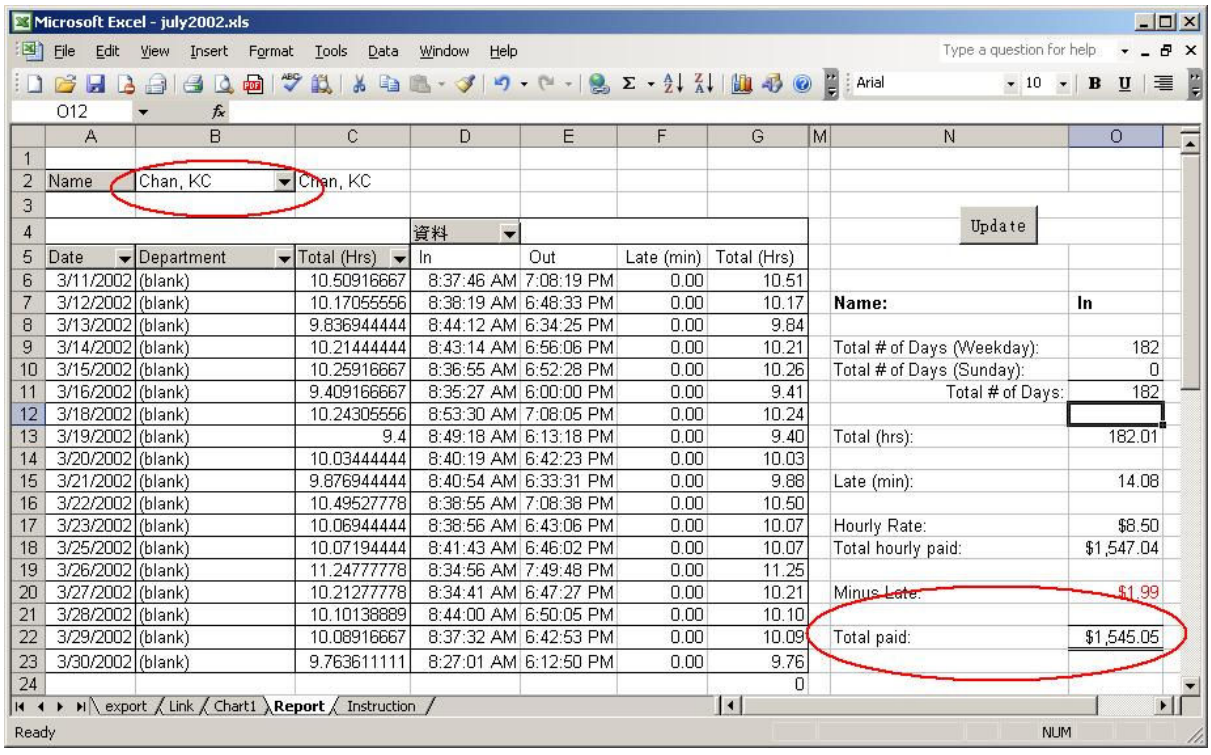
This section is for backing up and exporting the data to PC.

Exports (XLS)

The built-in reports, including the *Access Report*, *Attendance Report* & the *Daily IN/OUT Report*, can be exported to PC directly in the popular XLS format, which enables smooth integration with office suite applications such as Microsoft EXCEL. Various reports can then be easily generated using the built-in features of the office suite application. In this way, companies can design their own report formats that are best suitable to their existing operations.

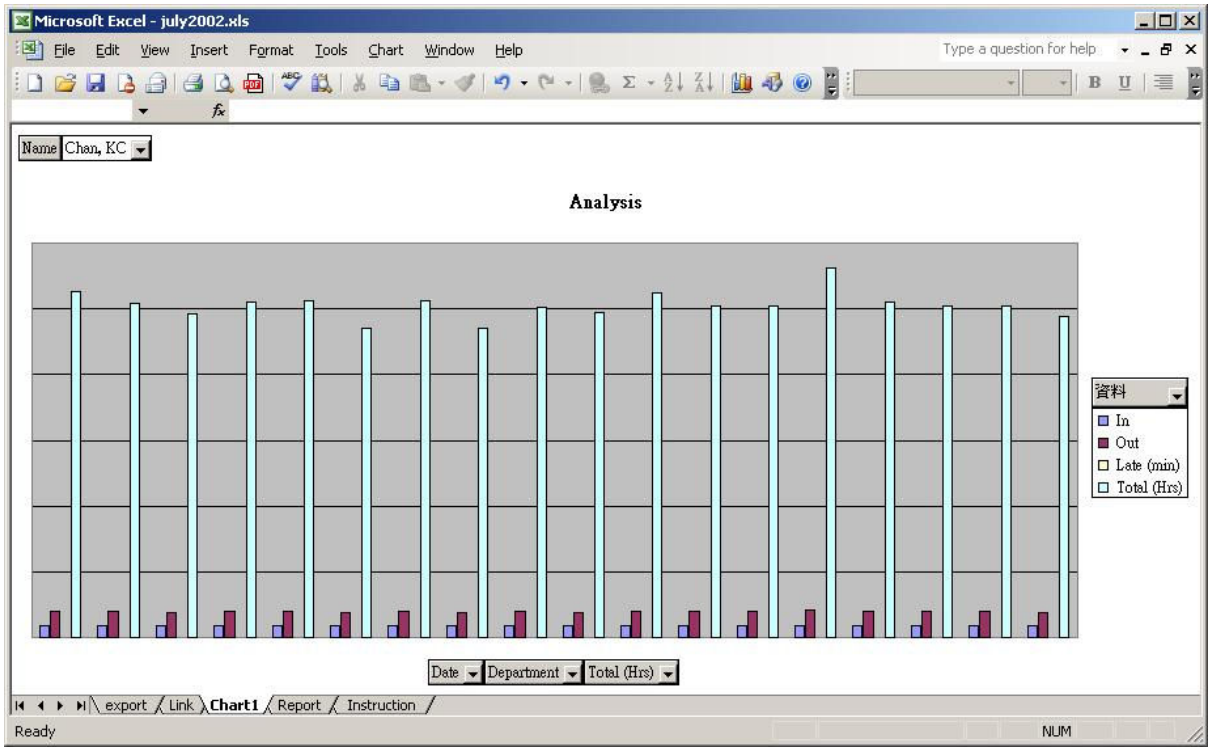


The following is a typical output example: -



	A	B	C	D	E	F	G
5	Date	Department	Total (Hrs)	In	Out	Late (min)	Total (Hrs)
6	3/11/2002	(blank)	10.50916667	8:37:46 AM	7:08:19 PM	0.00	10.51
7	3/12/2002	(blank)	10.17055556	8:38:19 AM	6:48:33 PM	0.00	10.17
8	3/13/2002	(blank)	9.836944444	8:44:12 AM	6:34:25 PM	0.00	9.84
9	3/14/2002	(blank)	10.21444444	8:43:14 AM	6:56:06 PM	0.00	10.21
10	3/15/2002	(blank)	10.25916667	8:36:55 AM	6:52:28 PM	0.00	10.26
11	3/16/2002	(blank)	9.409166667	8:35:27 AM	6:00:00 PM	0.00	9.41
12	3/18/2002	(blank)	10.24305556	8:53:30 AM	7:08:05 PM	0.00	10.24
13	3/19/2002	(blank)	9.4	8:49:18 AM	6:13:18 PM	0.00	9.40
14	3/20/2002	(blank)	10.03444444	8:40:19 AM	6:42:23 PM	0.00	10.03
15	3/21/2002	(blank)	9.876944444	8:40:54 AM	6:33:31 PM	0.00	9.88
16	3/22/2002	(blank)	10.49527778	8:38:55 AM	7:08:38 PM	0.00	10.50
17	3/23/2002	(blank)	10.06944444	8:38:56 AM	6:43:06 PM	0.00	10.07
18	3/25/2002	(blank)	10.07194444	8:41:43 AM	6:46:02 PM	0.00	10.07
19	3/26/2002	(blank)	11.24777778	8:34:56 AM	7:49:48 PM	0.00	11.25
20	3/27/2002	(blank)	10.21277778	8:34:41 AM	6:47:27 PM	0.00	10.21
21	3/28/2002	(blank)	10.10138889	8:44:00 AM	6:50:05 PM	0.00	10.10
22	3/29/2002	(blank)	10.08916667	8:37:32 AM	6:42:53 PM	0.00	10.09
23	3/30/2002	(blank)	9.763611111	8:27:01 AM	6:12:50 PM	0.00	9.76
24							0

Sophisticated graphical representation of the data for each user can then be generated as follows using the built-in Microsoft Excel's graphic functions:-



Note: Macro Programming is required in generating the above Microsoft Excel Reports. An example is available for download in the manufacturer's website (july2002.xls). Please consult the Microsoft Excel Operation Manual for more information.

Exports (TXT)

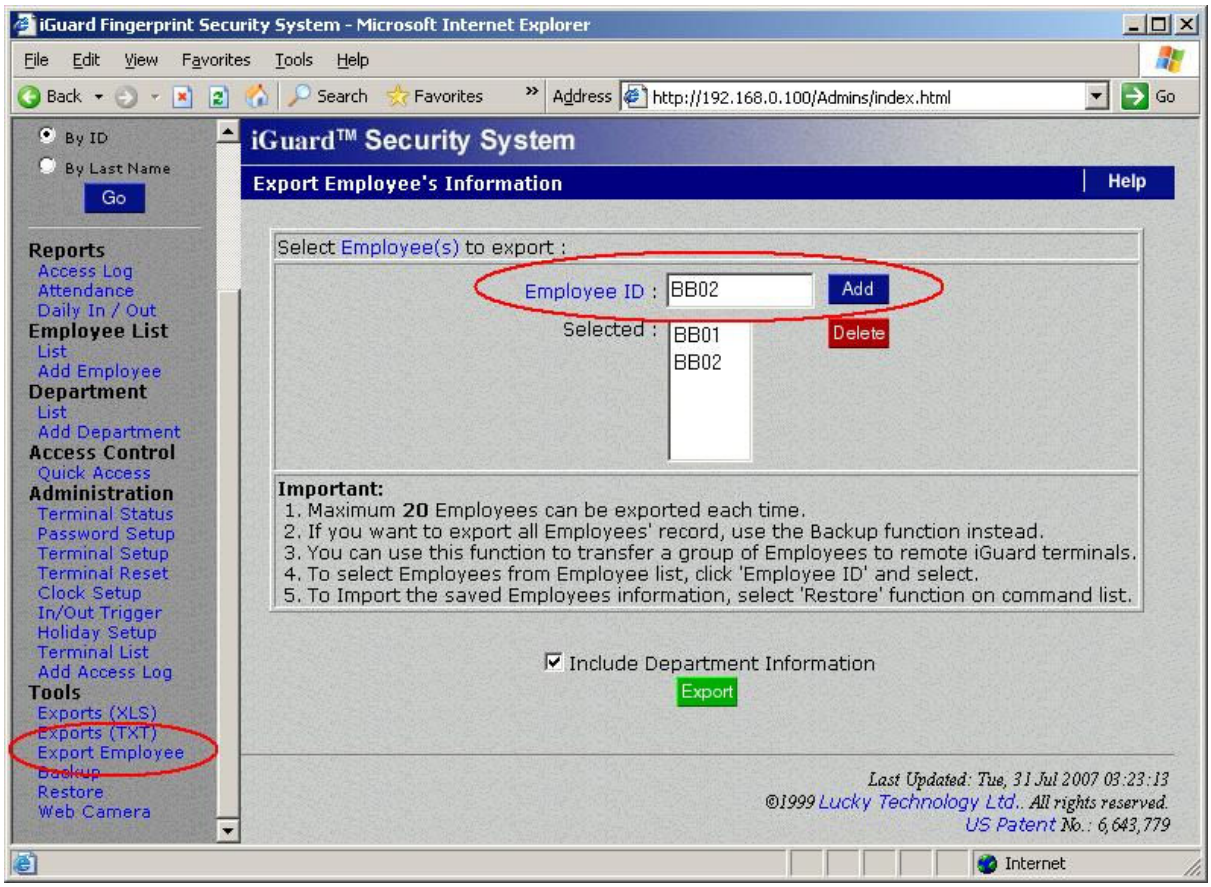
The *TEXT* file is useful for exporting to existing payroll programs used in the company.

The format of the text file is as follows:-

```
"Item","Employee ID","Name","Other Name","Date","Time","Terminal","In/Out"
"1","A1155","Shek, Ying Kuen","¥Û-^Åv","09/30/1999","20:02:04","F1103","Out"
"2","B1077","Yu, Andre","$E$®·R","09/30/1999","19:58:58","FLATB","Out"
"3","C001","Leung, Brian","±ç·ç°ò","09/30/1999","19:58:50","FLATB","Out"
"4","B1166","Chan, Chuen","³¯¬u","09/30/1999","19:56:45","FLATB","Out"
"5","A1174","Go, Kai Yin","§d±Ò½å","09/30/1999","19:52:30","F1103","In"
"6","B1082","Cheung, Moni","±i³ÍªY","09/30/1999","19:21:05","FLATB","Out"
"7","B1011","Leung, Wei Kun","±ç°û®Ú","09/30/1999","19:06:18","FLATB","Out"
"8","B1067","Lau, Ester","¼B¦pµØ","09/30/1999","18:58:11","FLATB","Out"
"9","A1154","Chow, Man Keung","©P¤å±j","09/30/1999","18:36:48","F1103","Out"
"10","A1050","Chan, KC","³¯°ê¬W","09/30/1999","18:20:59","FLATB","Out"
"11","A1002","Wong, Kit Ching","¶À¼ä-s","09/30/1999","18:19:07","F1103","Out"
```

Export Employee

Use this to selectively backup particular users' information from the internal user database to another device (instead of backing up the whole database).

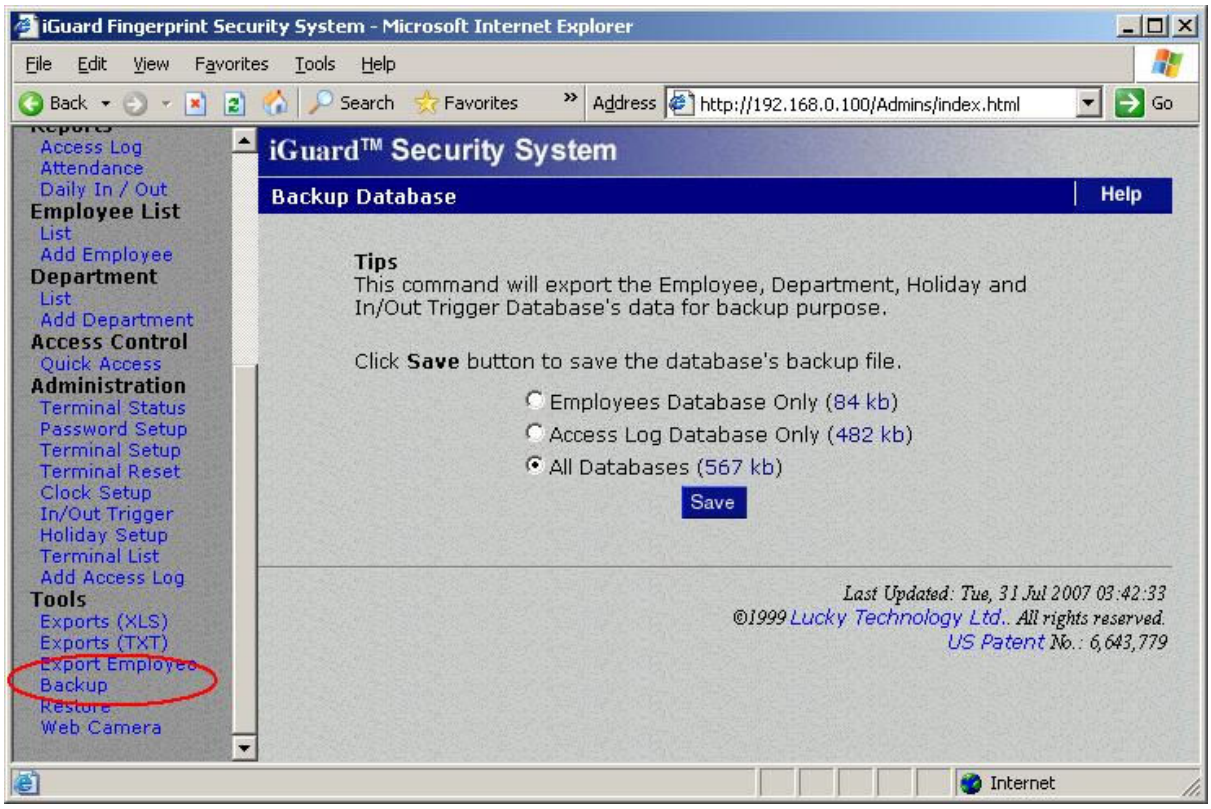


To include a particular user, enter the user ID in the *Employee ID* box and press the *Add* button.

Press the *Export* button to save the selected users' information in the file in the PC. This file can be later on restored to another iGuard, in order to avoid requiring these users to re-register. The restore procedure will be discussed below.

Backup

We recommend you backup the internal user data & access log regularly to the desktop computer. In the unlikely event that the system is to be replaced or the database file is corrupted, the old data can be restored back to the device, and the employees do not need to re-register.



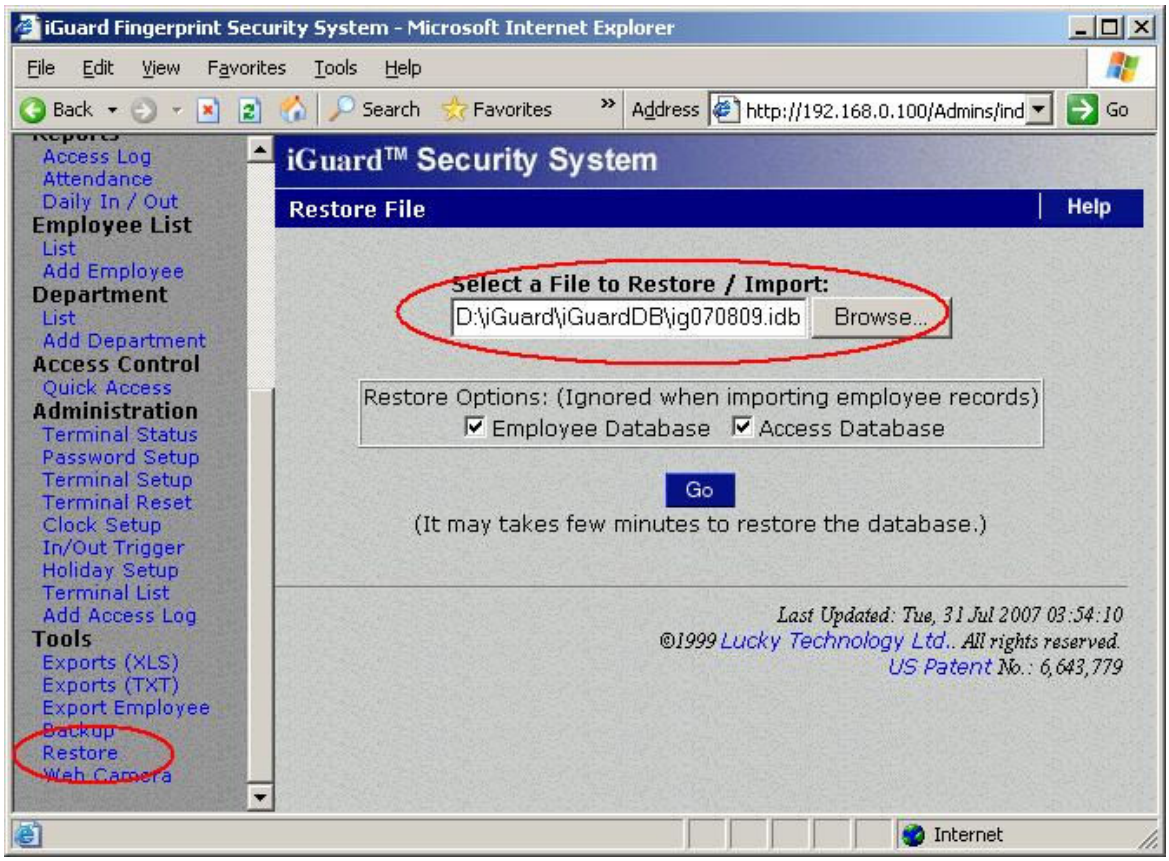
One can select to backup either the user database or the access log, or both. The size of each one is shown beside it in parentheses. Press the *Save* button to proceed. The following screen will appear:-

Press the OK button to save the database file

The default filename of the backup file is *igYYMMDD.idb*, where YY, MM & DD are the year, month and day of the backup date respectively for easy reference. If the *All Databases* option is selected, both the user database and the access log will be included in this single file.

Restore

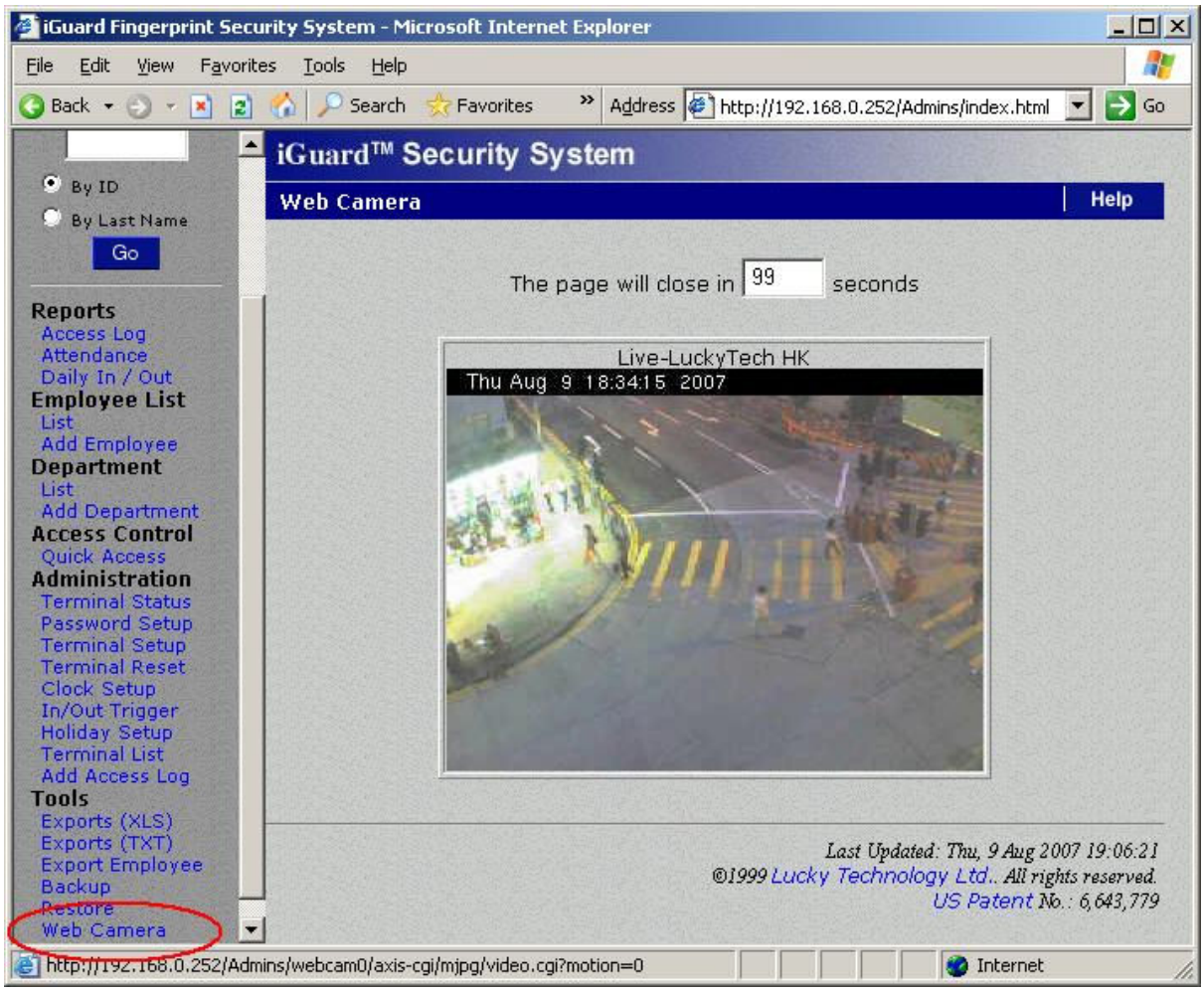
Use this page to restore the data from the backup file when it is necessary (for example, a new device has been installed), or to restore the exported file created in the *Export Employee* page discussed earlier.



One can choose to restore the user database only, the access log only, or both, by checking the corresponding checkboxes.

Web Camera

If the optional Web Camera is available to the network, iGuard can redirect the web camera's image to the browser as shown below: -



Please refer to the "*Administration → Terminal Setup"* page for more detail in setting up the web cameras.

APPENDIX

Fingerprint Enrollment

Fingerprint Enrollment is the process of registering the fingerprint template for later recognition.

A good enrollment is crucial for all fingerprint recognition systems in the market, including iGuard. A good fingerprint image captured during the enrollment process will significantly reduce the false-reject rate during later verification.

iGuard takes advantage of the advanced DFX (Difficult Fingerprint Extraction) technology, which works accurately with most people's fingerprint images, and iGuard can achieve an exceptionally low false-rejection-rate of less than 1%.

However, as individuals, our hands may have different levels of moisture. In some cases, iGuard may have difficulty in recognizing some users' fingerprint images (mostly the people with dry skin problems). The problem is more noticeable during the enrollment process since the device requires a more accurate and higher quality fingerprint image than the normal verification process.

The easiest way to get around the dry skin problem is to apply a small amount of moisturizing lotion on the dry skin during the enrollment process. *This step is only required in the enrollment stage, and will not be needed in the daily routine verification process.*

For users with wet skin problems, simply wipe the finger with cloth or paper towel before having any contact with the fingerprint sensor. Please note that excessive sweat *will* reduce the normal life time of the fingerprint sensor.

The image quality can be improved tremendously by taking care of the dry and wet skin condition discussed above. It is important that the user stores a high quality image during enrollment, because this is the fingerprint image that the device will use to compare against the submitted fingerprint images in all the verifications later on. If the users' enrolled fingerprint image is of low quality, the user may get unexpected results during the verification stage later on.

In the case of poor fingerprint quality or dry finger, iGuard will ask to lower the matching security for the particular user. A low security level can be more convenient to the user by reducing the false rejection rate, but it comes with a minor reduction in security level. Therefore, we recommend choosing low security level only for time attendance applications.

These are some of the error messages that may appear during fingerprint enrollment:-

Description	***LCD Display***
1. This message will appear during enrollment if the fingerprint is too dry. Try to lift up the finger and put it back on the sensor again. If the problem still exists, consider applying some skin moisturizing lotion as discussed above.	`Scanning 1 of 1` `=== Too Dry! ===`

2. This message will appear at the end of the fingerprint enrollment process if the fingerprint quality is only marginally acceptable, and suggests setting the security level to low for this particular user. Select *YES* to set it to Low. This security level can also be changed in the employee webpage later on.
scrolling message →
	`Set Security to`
	`Yes/No (1/2)? _`
	⋮
	⋮
	`Security to Low`
	`Yes/No (1/2)? _`

Here are some other general factors that may influence the enrollment:

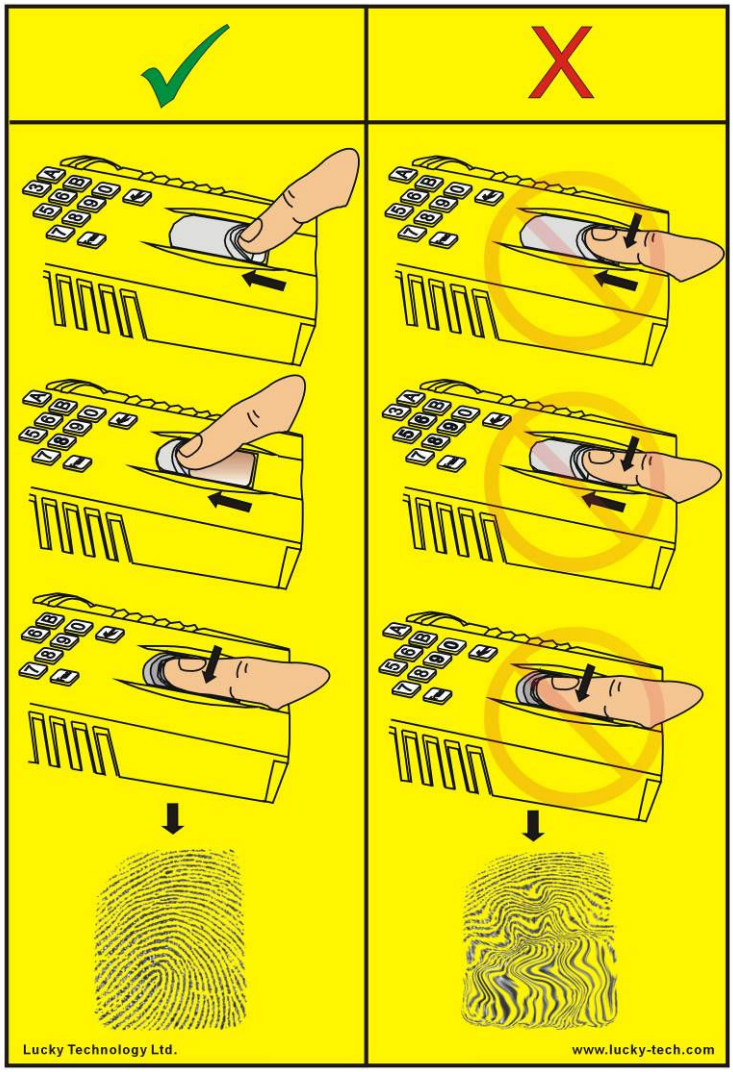
- **Finger Position**. Always align the center of the fingerprint with the center of the fingerprint sensor. Do not use the tip of the finger, and do not place the finger too much to the left or to the right. Otherwise, false reject may occur.

- **Finger area**. It is best to cover the sensor area completely with the fingerprint to ensure the maximum fingerprint surface contact area. A common mistake is to touch the sensor with the tip of the finger, which contains too few minutiae points. It is also best to use the thumbs rather than other fingers.

- **Finger rotation**. Keep fingerprint rotation minimal during the enrollment. The rotation should be within +/-10 degrees during enrollment.

- **Finger pressure**. Use medium pressure. Excessive pressure may distort the image and may adhere ridges together. Too little pressure will lead to a small fingerprint area or dry fingerprint.

Also, to avoid reading a blurry and smeared image, do not slide your finger across the sensor, as illustrated in the following diagram:

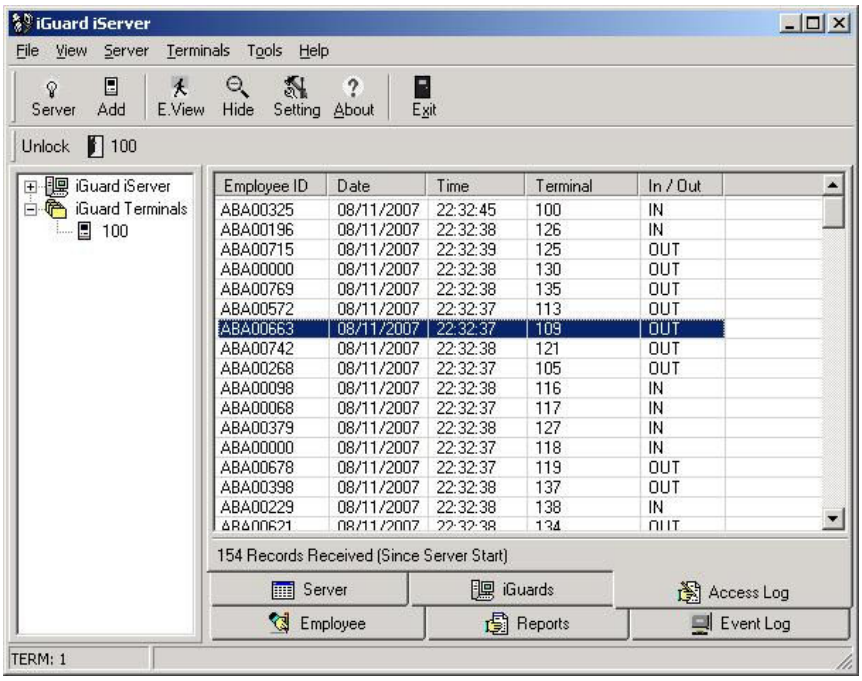


iServer

iServer is a Windows-based program that runs on PC for permanently storing the access log in the PC in a real time manner. It can be downloaded free of charge at the manufacturer's website.

Due to the limited memory, iGuard only keeps the most recent 10,000 access log entries only in its internal memory, using the First–IN–First–Out (FIFO) rule. By using iServer, all the access log entries can be saved permanently in the PC, and it is only limited by the available hard disk space of the PC.

The following is the iServer program running on a PC:-



The left panel shows the iGuards that are currently connected to the iServer program. In the above example, only one iGuard (ID:100) is connected, and this iGuard will send all the access log entries to the iServer program in real-time. Multiple iGuards can be connected to the same iServer program.

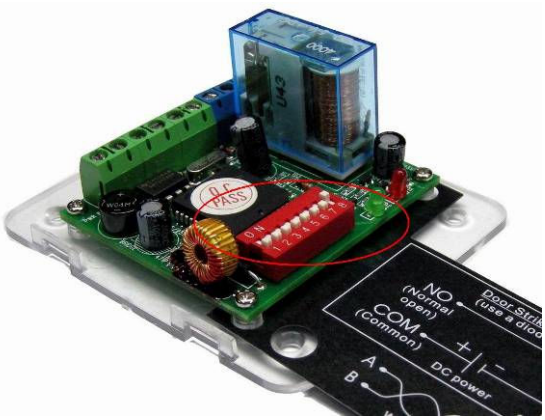
The right panel shows the recent access log entries in real-time.

By default, iServer stores the access log records in ODBC database format using Microsoft Access. iServer also supports other ODBC compliant database other than Microsoft Access, such as MS SQL, mySQL and Oracle.

Please refer to the operation manual that comes with the iServer utility for installation and operation.

Remote Door Relay

The iGuard capabilities can be enhanced by the use of the Remote Door Relay, which is sold separately from the iGuard unit. The Remote Relay assures that malicious damage to or tampering with the iGuard does not result in a release of the electric door strike or magnetic lock.



This device is to be physically installed inside the premises, and it is connected to the iGuard's *Remote Relay* connector at the back of the unit through a special twisted-pair cable. When using the relay, the electric door strike actions are controlled by the remote door relay rather than directly by the iGuard unit. The remote relay will only release the strike / lock when a properly addressed Release-and-Relock signal is received from the iGuard unit to which it is attached.

The use of the relay is recommended for all access control installations, and is required when controlling a 12VDC electric door strike or magnetic lock with a current rating above 1Amp.

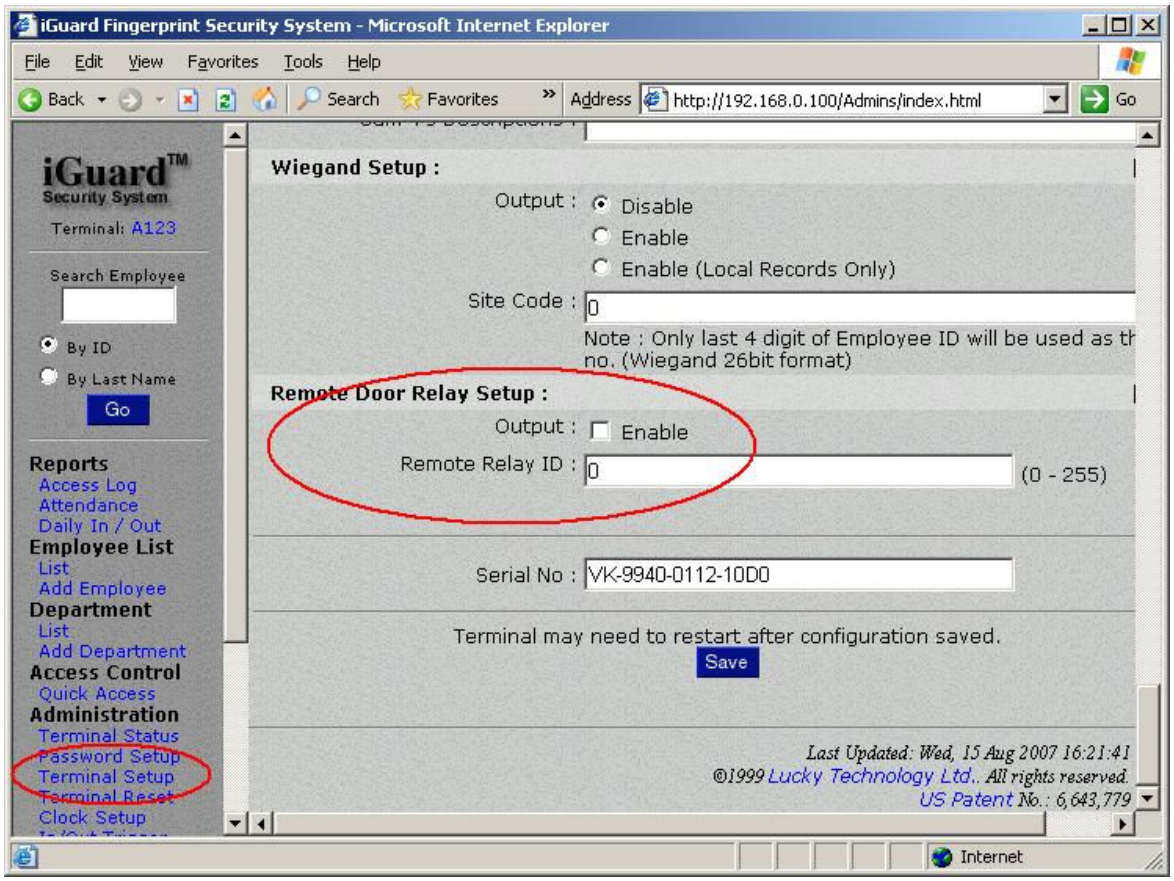
Configuration

Before installing the relay, set the Remote Relay ID with the 8-Bit Jumper switches on the relay (circled in red in the above picture). The chart below explains how to calculate the value that the switches are set to. Add the Numeric Value of each switch you turn to the 'On' position. This total will be the ID value of the Relay.

Switch Number	Numeric Value
1	1
2	2
3	4
4	8
5	16
6	32
7	64
8	128

For Example, if the switches 3 and 7 are turned to 'ON', the value is 68 (i.e., 4 + 64 = 68). If all switches are turned to 'ON', the value is 255.

The same ID must ***also*** be specified in the webpage as shown in the screen shot below, and the *Output Enable* checkbox must also be checked.



The following is the connection terminals of the Remote Relay:

Terminal	Label	Description
1	NO	Door Relay's Normal Open
2	COM	Door Relay's Common
3	NC	Door Relay's Normal Close
4 & 5	DOOR SW	Door Switch
6	A – RS485	Connect to iGuard
7	B – RS485	Connect to iGuard
8	+12V DC	+12V DC
9	GND	Power Ground

Care must be taken when connecting the two twisted-pair wire to the devices, and do not mix up the two labels, A & B, and the corresponding terminals of the Remote Relay device.

Warning: A twisted pair of wire must be used to connect the iGuard and the Remote Relay device. Otherwise, the wire may pick up the noise in the environment (such as the noise generated from the power wire nearby), and may make the device malfunction.

SuperMaster

SuperMaster is a device for supporting up to 20,000 users. It is used to replace the normal Master unit, which supports a maximum of 1,000 users only.

The operation of the SuperMaster is very much like the normal Master unit, except that it does not perform any user authentication itself. It acts like a file server that serves the requests for user information from all the slave units, and to centrally save the access log records from all the units.

Follow the same setup procedure to configure the network and other settings of the SuperMaster.

Similar to the normal master / slave configuration, the slave unit connects to the SuperMaster by specifying the IP address and the Port number of the SuperMaster, in much the same way as connecting to a normal Master unit.

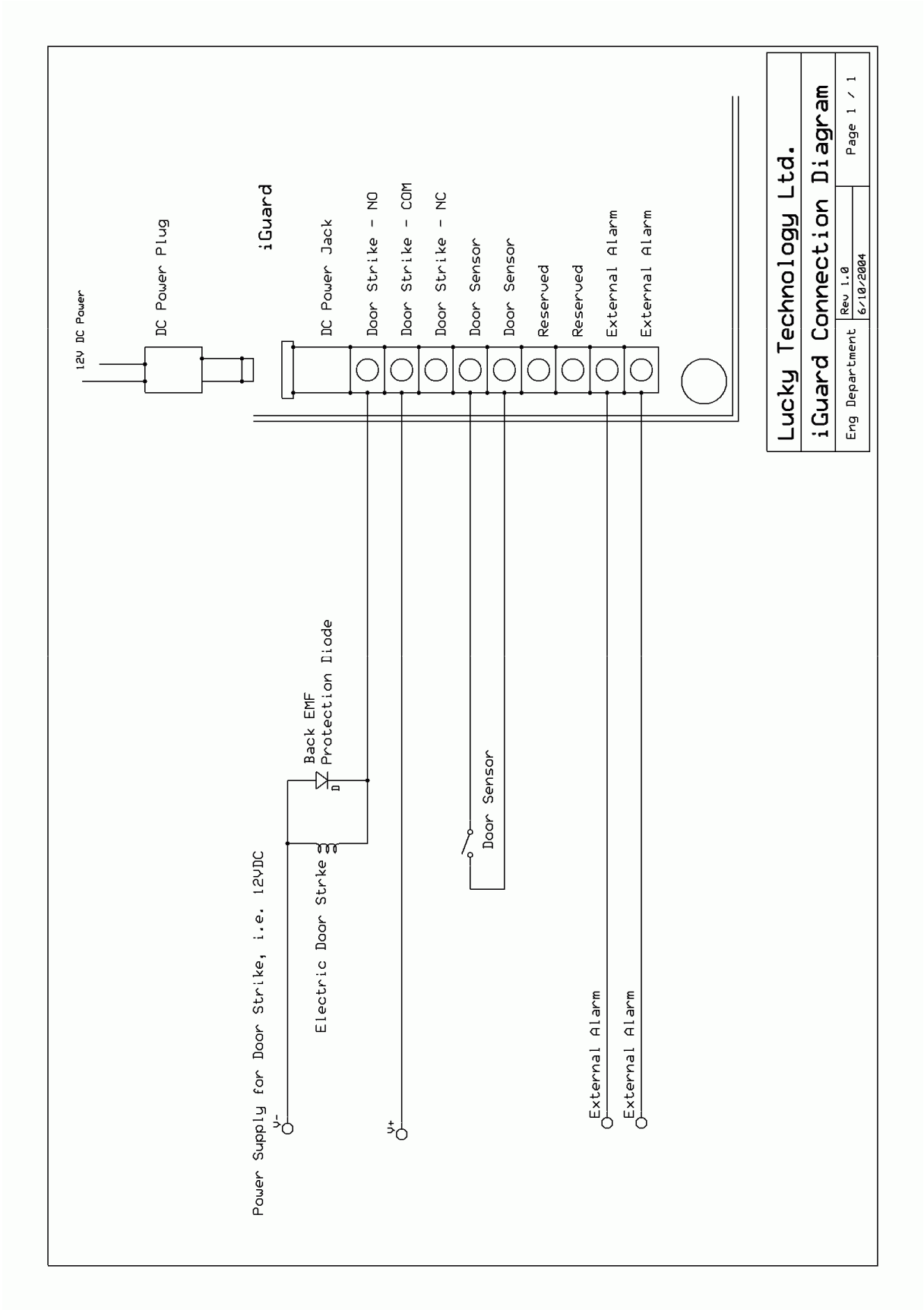
Unlike the normal Master unit, the SuperMaster does not synchronize the whole user database to the slave units. Instead, it intelligently selects a maximum of 1,000 users from the internal user database (which may contain as many as 20,000 users), and upload these users to each slave unit.

During the normal verification procedure at a slave unit, the slave unit will first search its internal database to see if the user information is already available. If so, the slave unit will continue the verification process normally. Otherwise, the slave unit will send a request to the SuperMaster in the background for the user information, and continue the process after receiving the information from the SuperMaster.

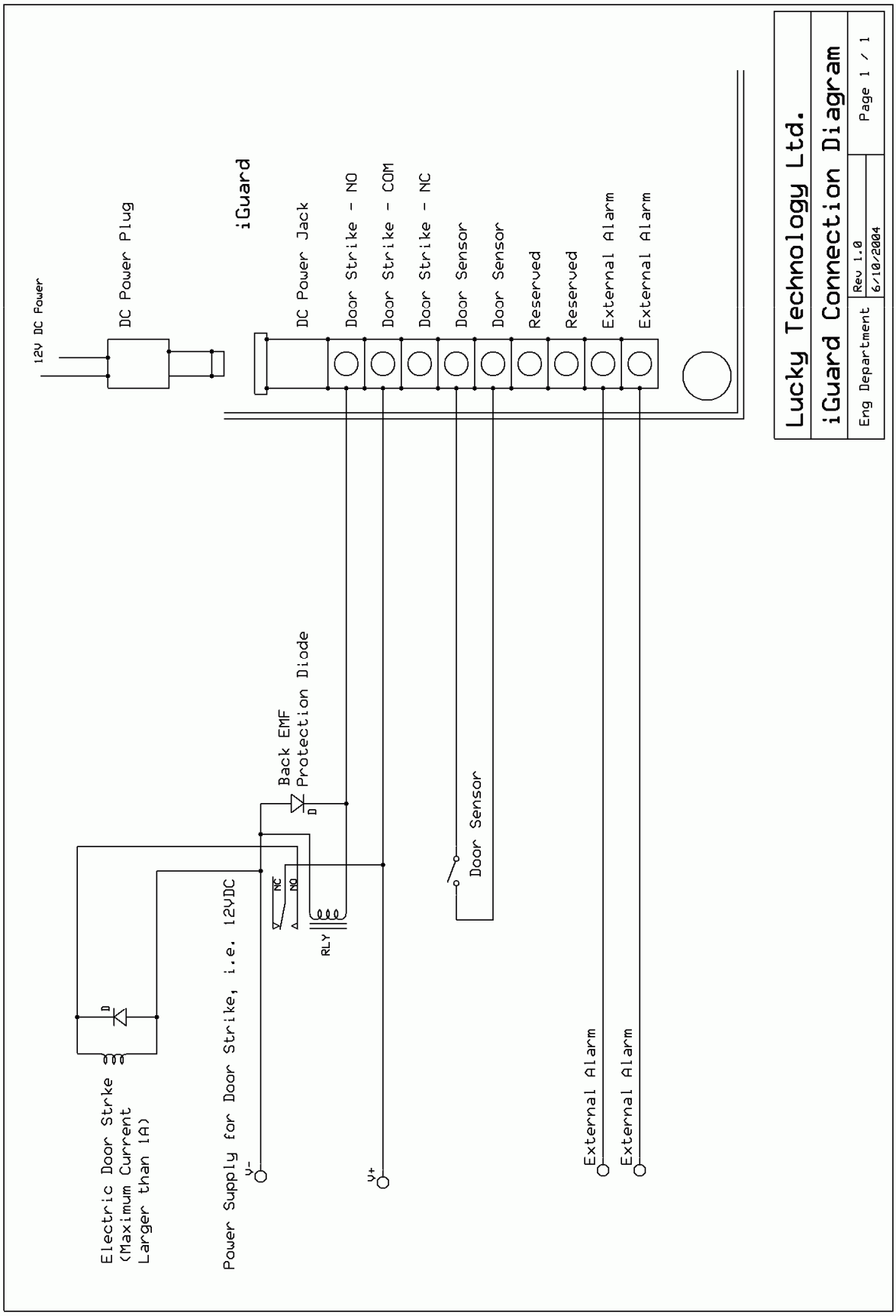
The slave unit will keep the most recently accessed 1,000 users in its internal user database, and the oldest user information will be replaced by the newly received user information. Therefore, in case the network connection is lost, chances are pretty good that the user can still get authenticated in these slave units, unless the user is not one of the 1,000 recent users.

Connection Diagram

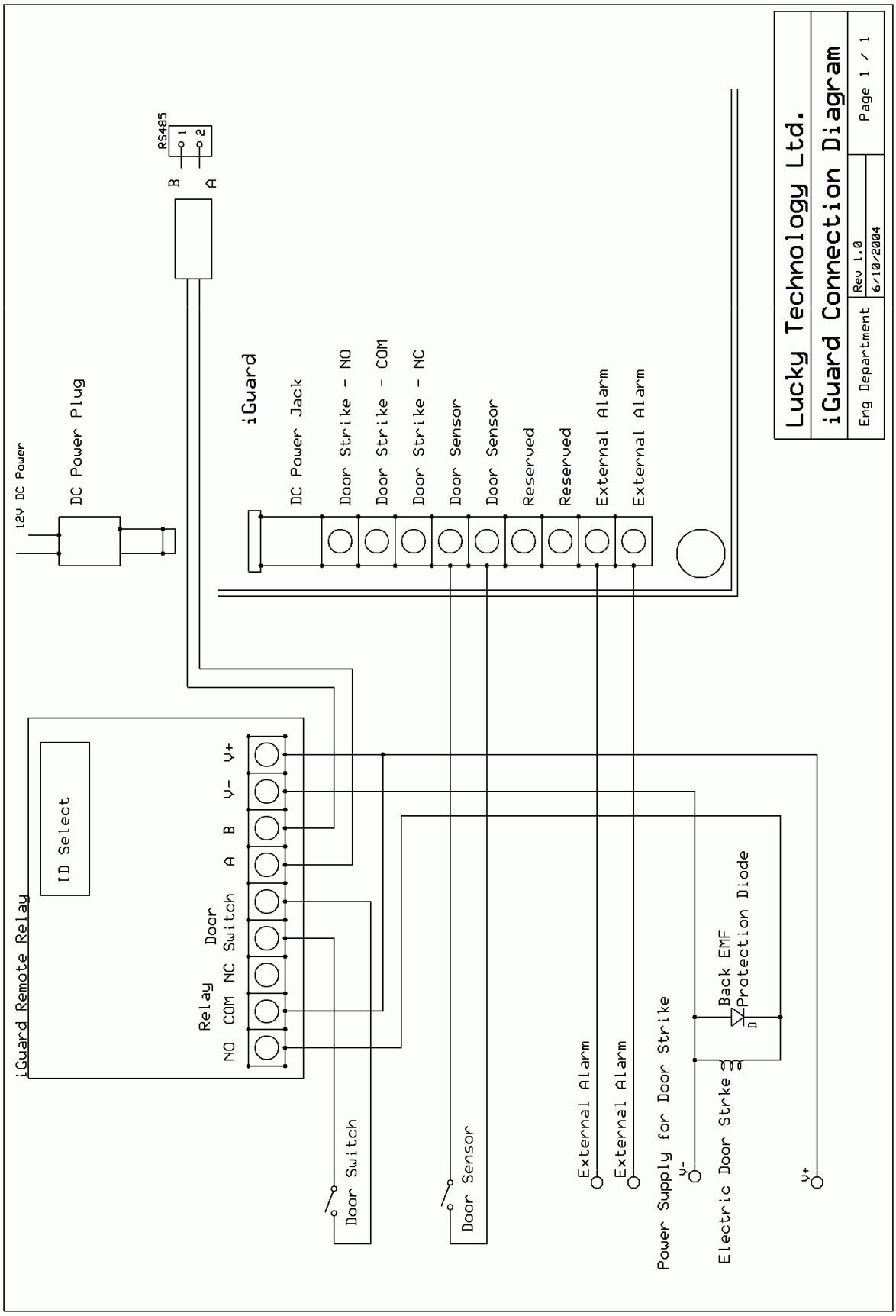
Basic Connection



Basic Connection (Large Load)



Remote Relay



iGuard Part List

LM Series Readers	
LM520-SC	Smart Card reader with Embedded Web Server (1,000 users)
LM520-FSC	Finger print scanner / smart card reader with embedded Web Server (1,000 users)
LM Series Super Master (Master Only)	
LM-SM-5000	Super Master unit licensed for up to 5,000 users. Stores 10,000 finger print templates and 20,000 transaction records.
LM-SM-10000	Super Master unit licensed for up to 10,000 users. Stores 20,000 finger print templates and 20,000 transaction records.
LM-SM-20000	Super Master unit licensed for up to 20,000 users. Stores 40,000 finger print templates and 20,000 transaction records.
Special Promotions	
LM520-FSC-SP	Finger print scanner / smart card reader with embedded Web Server (1,000 users, Master only – cannot be configured as slave)
LM-FSC-SAM	Demo Unit (Not for resale). Finger print scanner and smart card reader with merged database (1,000 users). Power supply included.
LM-SM-SAM	Demo Unit (Not for resale). Super Master unit licensed for up to 5,000 users. Stores 10,000 finger print templates and 20,000 transaction records. Power supply included
Smart Cards	
CSC-1K	Mifare 1k Classic smart card formatted for use with iGuard®.
Accessories	
IG-PWR	12VDC switching power supply with DC plug for use only with iGuard®.
IG-PWR-CAB	Power supply cable with DC plug for use only with iGuard®
IG-ER-01	Remote Door Relay
Replacement Parts	
LM520-FP-RD	Daughter board for LM520-FSC complete with sensor, LCD and casing.
LM520-RD	Daughter board for LM520-SC with LCD and casing.
LM520-C	Casing for LM Series iGuard® units with shutter and spring.
LM520-K	Keypad for LM Series iGuard® units.

Contact Information

Lucky Technology Inc. (America)

Address: 5th Floor, 7380 Sand Lake Road, Orlando, FL 32819
Telephone: 800-410-6798 (Sales)
800-441-6798 (Technical Support)
Fax: 800-486-6798
Email: sales@lucky-tech.com (Sales)
tech@lucky-tech.com (Technical Support)

Lucky Technology Ltd. (Eurpoe)

Address: Levels 2, 3 & 4, Edouard VII, 17 & 23 Square, Paris 75009, France
Telephone: +33 1 5343 5172
Fax: +33 1 5343 9292
Email: sales@lucky.com.hk

Lucky Technology Ltd. (China)

Address: Level 6, Tower W2, Oriental Plaza, 1 East Chang An Avenue
Dong Cheng District, Beijing 100738, PRC China
Telephone: 86-10-8520-0386
Fax: 86-10-6251-2009
Email: saleschina@lucky.com.hk

Lucky Technology Ltd. (International)

Address: 2/F, Flat A-D, Wah Hing Industrial Mansion, 36 Tai Yau Street
San Po Kong, Kowloon, Hong Kong
Telephone: 852-3176-6056
Fax: 852-3012-1980
Email: sales@lucky.com.hk

Website: www.lucky-tech.com

# # # # #

Notes:

Notes:

Lucky Technology Ltd.

www.lucky-tech.com